PCT/CA 10040018 31
11 FEBRUARY 2005 11-02-05

PA 1274274

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

January 26, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: ***60/511,790***
FILING DATE: ***October 16, 2003***

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

E. BORNETT
Certifying Officer

BEST AVAILABLE COPY

11696 U.S.PTO

PTO/SB/16 (08-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No. ER 458455995 US

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Rene	Juneau	Thornhill, Canada

Additional inventors are being named on the 0 *separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max)

METHOD FOR DETECTING AND PREVENTING UNAUTHORIZED SIGNAL USAGE IN A CONTENT DELIVERY NETWORK

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☐ Customer Number:

OR

☑ Firm or Individual Name	Rene Juneau				
Address	155 Westhampton Drive				
Address					
City	Thornhill	State	Ontano	Zip	L4J 7X2
Country	Canada	Telephone	905-669-0279	Fax	

22387 U.S.PTO
60/511790
101603

ENCLOSED APPLICATION PARTS ***(check all that apply)***

☑ Specification *Number of Pages* 26
☑ Drawing(s) *Number of Sheets* 14
☐ Application Date Sheet. See 37 CFR 1.76
☐ CD(s), Number
☐ Other (specify)

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☑ Applicant claims small entity status. See 37 CFR 1.27.
☐ A check or money order is enclosed to cover the filing fees.
☐ The Director is herby authorized to charge filing fees or credit any overpayment to Deposit Account Number:
☑ Payment by credit card. Form PTO-2038 is attached.

FILING FEE Amount ($)

US$80.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☑ No.
☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

SIGNATURE

TYPED or PRINTED NAME Rene Juneau

TELEPHONE 905-669-0279 or 416-806-0122

Date October 15. 2003

REGISTRATION NO. *(if appropriate)*

Docket Number:

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop Provisional Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Provisional Patent Application of
René Juneau
for

TITLE: METHOD FOR DETECTING AND PREVENTING UNAUTHORIZED SIGNAL USAGE IN A CONTENT DELIVERY NETWORK

CROSS REFERENCE TO RELATED APPLICATIONS Not Applicable

FEDERALLY SPONSORED RESEARCH Not Applicable

SEQUENCE LISTING OR PROGRAM Not Applicable

BACKGROUND OF THE INVENTION—FIELD OF INVENTION

This invention relates generally to the detection of unauthorized signal usage in a content delivery network, and more particularly to the detection of unauthorized signal usage for content distributed by way of wired or wireless networks to subscriber receiving devices. By way of examples, the present invention may be deployed in conjunction with various subscriber receiving devices such as television set-top boxes, television and audio receivers, personal computers or personal digital assistants, mobile telephone handsets or other handheld communication devices and the like. Moreover, the present invention may be used to detect unauthorized signal usage in relation to numerous categories of deliverable content, whether in the form of voice, video, sound, executable applications, data or the like , including any combinations thereof.

BACKGROUND OF THE INVENTION

Distribution networks

FIG.1 shows a typical television digital television distribution system for a cable or satellite television system, which will be referred to hereafter as the *network*.

Components of the network 10 could reside on a single physical system or on separate systems linked by one or more communication networks. Multiple instances of each component may also be required. The network 10 includes a plurality of content providers from external sources 11a as well as internal content 11b produced by the network operator. The content consists of audio, video, data, applications, or any combination of all of these, that is made available to receivers by broadcast or point-to-point transmission or requests.

Examples of content streams include television signal with audio, video, closed captioning and interactive applications all embedded into a composite signal, as would be the case with a television signal supporting the Wink or WebTV interactive television specifications; a series of separate digital transport streams for audio, video, interactive television, and conditional access. A given content may be shared by one or more services. For example, an English language service may be defined as containing a given video stream and an English-language audio stream. A Spanish service may be defined using the same video stream and a Spanish-language audio stream. In this manner, only the bandwidth of one video stream is used on the system while providing two separate channels on a program guide.

Content may be received in a format that is compatible with the operator's network, or may require processing before transmission. Examples of processing include compression and encoding for video and audio signals, format conversion, and encryption or the signals. Content may also be available from one or more content servers 11c at the operator site. Content from the server may be transmitted in real-time, or slower or faster than real-time for purposes of caching content for deferred viewing.

The content may flow into encoders 12 which process the content prior to distribution, or, for content that is already encoded, directly into multiplexers. From the encoders, the processed content flows into a multiplexer 13 for delivery, through a network interface 14 to one or more communication networks 15 for delivery to a plurality of receivers 16. The communication network may provide multiple facilities for communication between the receiver and the control networks. As examples, on a cable television network, bandwidth may be allocated separately for content transmission, control signal transmission, and return communication from a receiver with all communication occurring on the same cable. On a satellite television system, the content and control signals are transmitted over the satellite, while the receiver may communicate back to the network through a telephone connection.

Along with the content from content providers 11, various forms of data are transmitted to aid the viewer in the use of a multi-channel, multi-service system. This type of information, which can include the electronic program guide and related tables for access, frequency and other information for receiving and describing the signal, are known as service information (SI) tables. SI tables are produced and transmitted by the SI generator 17, and can also include various forms of control information from external sources to control access for content like subscription services and pay-per-view movies, and other forms of information on the content that may be of use to the receiver 16.Signal enhancements such as station logs, data, and other forms of content may be included with the content from the various sources, may be added to or removed from the content by an injector or filter 19 that occurs before the encoding process, or by and injector or filter that occurs after the encoding process.

Security and authorization may be provided by a conditional access system 20 (CA). The CA determines which content the viewer is allowed to access. The CA can include a content coding system 24 for protection of the content during transmission, permission management 21 for control of authorizations on a per user or receiver basis, content management 22 for controlling access to content, message encryption 23 facility to secure the communication authorization and other messages for transmission, and a receiver conditional access system 26 for communication with the operator's CA and local secure storage of permission and content access information. The content coding system 24 may perform various transformations on all or part of the content signal to prevent unauthorized access, including signal modification, encryption, and other methods.

Subscription control is typically managed by entering service authorization and cancellation commands on the subscriber management system (SMS) 25. The SMS forwards the subscription control requests to the CA system, which generates the appropriate commands and operations to ensure to deliver subscription control commands in the form and manner required to be effective on the receiver.

In a typical cable television system, the communication network 15 is the system of amplifiers, transmitters, re-transmitters, copper cable, fiber optic systems, switches and routers used for distribution of the signal. The receivers 16 are connected to the cable

network, and communicate back with the operator using Internet, DAVIC (Digital Audio Video Council, Geneva, Switzerland) and/or other command protocols supported by the communication network 15.

Other examples of the communication network 15 include DTH (direct to home) satellite or microwave multichannel multipoint distribution service (MMDS), local multipoint distribution system (LMDS) television distribution system, DSL (Digital Subscriber Loop) and its various high-speed variants as used, for example, by telephone companies for high-speed data and video transmission, ATM (Asynchronous Transfer Mode) networks, cellular telephone and communication networks, and others.

Receivers

FIG. 2 depicts the functional components of a typical digital television receiver on the network 10. The components may be implemented in hardware or software. Individual or groups of functions may be provided by separate applications communicating through an operating system or other shared facility, or may be part of a single application.

Typical components of a receiver are one or more network interface 41 for communication to and from the operators' network(s). In a television receiver, interfaces may consist of one or more tuners to receive signal from the network, and a network interface such as a modulator or a telephone modem for returning data to the network. On a digital receiver, demodulate/demultiplex functions 42 convert analog signals into digital data, and extract the data required from the stream. A decrypter function 43 performs decryption functions on the signals, and is typically controlled by the receiver CA subsystem (RCAS) 26. The decryption may be based on analog or digital means of preventing unauthorized access to the signal. On a digital receiver, the decoder 45 transforms the signal bits into the content format required by the viewer. For example, a decoder would convert the bits from MPEG digital audio and video bit streams into analog television signals.

RCAS 26 controls which content may be accessed. Examples of control mechanisms include channel subscription authorizations received from the CA, and pay-per-view purchases made at the receiver. The RCAS 26 can determine whether access is allowed through its own locally stored parameters, or by making an authorization check with the CA 20.

One or more processors 50 are used to implement the functions of the receiver or to provide or control communication between the functions. The functions and facilities of the receiver may further be controlled by an operating system that executes on one or more processors.

Optional functions available on a receiver can include an electronic program guide (EPG) 51 to allow the user to list, select and obtain other information on the content available; an interactive television (iTV) subsystem 52 to provide facilities for executing other applications such as games, viewer response gathering and others. These iTV applications may operate in conjunction with television programs, or independently as separate services. Other applications 53 include system configuration, audience measurement, targeted advertising delivery and others. Applications such as the EPG and the other applications may in turn be iTV applications that use the facilities of the iTV subsystem 52. Other applications 53may also include capabilities for exercising some control over what can be viewed, such as parental control and copy protection. These applications may in turn require network components that may be implemented in one or more of the injector/filter 18 or 19, content spooler 11c, CA 20, SI Generator 17 or other component.

Multiple instances of each functional component may be available on a receiver. This would allow simultaneous processing of multiple signals, or the ability to handle different signal types. Examples include the ability to process to television signals at a time for picture-in-picture functions, or for recording one program while watching another on a receiver equipped with a personal video recorder (PVR) feature, and the ability to receive analog and digital signals.

Functions and applications can be provided and managed in multiple ways. The applications may be part of the software on the receiver, and included with the original or updated software; one or more separate binary applications transmitted separately to the receiver; or interpreted applications that are executed within an iTV environment. The iTV applications may be considered separate content, or may be included with video or other content as optional enhancements. Transmission of an application may be managed may as a separate content stream or as a component of a video program. In some cases, functions or the receiver such as the EPG are implemented as iTV applications.

Other examples of receivers include any or all of the following operating alone or in combination: digital set-top cable and satellite receivers; integrated components within digital televisions; personal computers with appropriate network connections, cellular telephones and personal digital assistants (PDAs) connected through wireless networks and occasional computer network hook-ups, and gaming consoles.

More and more of such receiving devices may rely on CA systems similar to those used in television transmission, including satellite and other digital radio systems, , mobile telephones using chip-card technology,, and mobile or home devices and related services for receiving music, video or other content that receive content either directly from a network or indirectly through a computer such as the iPod™ music player and iTunes™ music service from Apple Computer Inc, Cupertino, CA..

Other types of receivers and systems have the ability to receive software updates and applications through their respective networks. In television and other receivers, these applications do not necessarily require interaction with the user, as they may execute in the background without the user's knowledge.

Receivers may include an application execution environment to receive and execute scripts or compiled or interpreted applications. Examples include the various Java systems such as Personal Java, Java TV and others from Sun Microsystems, Inc., Santa Clara, CA, and its licensees, as implemented in computers, web browsers and other devices. In television receivers, application execution environments include iTV products and specifications such as WebTV and MSN™TV services from Microsoft Corporation, Redmond, WA, the Wink system from Wink Communications, Alameda, CA, the OpenTV system from OpenTV Inc., San Francisco, CA, and specifications such as DVB-MHP from the DVB Project, Geneva, Switzerland, and OCAP (Open Cable Application Platform) from the Society of Cable Telecommunications Engineers (SCTE), Exton, PA and others. Other applications, such as an EPG, an audience measurement application, a targeted advertising delivery system, or others may be implemented as applications within an application execution environment, or may include an application execution environment which may provide similar capabilities to an iTV system for running interactive or background applications. Other systems with similar capabilities are known to those of skill in the art.

Control issues with networks and receivers

In the particular case of television distribution systems, whether using analog, digital of a combination of both technologies, network and receiver components rely on the encryption and access control components of the CA systems. These CA systems control which receivers have access to which content and signals, whether in the form of specific viewing channels, program selections, or other features available to the subscriber such as interactive applications. Examples of these security systems include the Simultcrypt specifications developed by the DVB Project, Geneva, Switzerland, conditional access systems and smart cards from Nagravision SA, Cheseaux, Switzerland, and NDS Group plc, Middlesex, UK, and the conditional access subsystems of the DigiCipher™ II products from Motorola , Inc. , Schaumburg, IL, and the PowerVu™ products from Scientific-Atlanta, Inc. Lawrenceville, GA. Several other systems for controlling or facilitating access have been implemented, examples of which include using parental control methods such as the V-Chip technology offered by Tri-Vision International LTD, Toronto, Canada, the electronic program guide (EPG) products offered by Gemstar-TV Guide International, Inc., Los Angeles, CA, video copy protection products from Macrovision Corporation, Santa Clara, CA.

These and other systems have been described in the following United States patents:

• 4,461,032	June, 1982	Skerlos	725/25	CA
• 4,510,623	July, 1982	Bonneau et al.	725/27	CA
• 5,146,496	June, 1991	Westerfer et al.	380/213	CA
• 5,224,161	July, 1991	Daniel et al.	380/239	LEREA/crypt
• 5,880,769	April, 1995	Nemirofsky et al.	725/139	Smart card
• 5,970,206	April, 1997	Yuen et al.	386/83	Gemstar/EPG
• 6,067,440	June, 1997	Diefes	725/27	CA for switched
• 5,485,518	Sept., 2003	Hunter et al.	725/28	Parental control
• 5,828,402	Dec., 1996	Collings	725/28	V-CHIP
• 5, 438, 620	Aug., 1995	Ryan et al.	380/218	Macrovision.

CA systems typically include components at the network operator's site and within the receivers, as described in FIG. 1 and FIG. 2.

The CA system at the network operator site communicates authorizations to a receiver CA subsystem (RCAS) located on each receiver. The receiver, its RCAS, or a component or subsystem peripheral to the RCAS such as a smart card, typically has one or more identifiers. These identifiers, alone or in combination, may be used for the CA or other systems to communicate with or send authorization commands to the RCAS or other components or subsystems of the receiver. These authorizations are typically based on transmitting one or more authorizations to a receiver; on a receiver requesting a list of authorized services; or, for services such as pay-per-view movies, on a credit scheme, where the credit is transmitted to or provided with the receiver, and said credit is reduced through usage of pay-per-view content. The credit may be based on a financial amount, a number of tokens or other methods that are known to those of skill in the art.

The CA systems may not provide facilities for a large number of operators to enter authorizations or to manage billing and other customer-oriented functions. Likewise, known CA systems may not provide for the handling or interfaces for the handling of large volumes of transactions, whether by batch processing or scripting. Where such facilities may be provided within a CA system, the operators may not be accustomed to using them, as they

may not provide convenient or easily usable interfaces, and they may not include logging and other audit trail mechanisms. Functions are typically provided by a subscriber management system (SMS), which in turn passes the authorization request to the CA system for processing and transmission to the receiver. Examples of SMS include systems provided by DST Innovis, Inc., El Dorado Hills, CA, CSG Systems, Incorporated, Englewood, CO, and others.

CA systems are typically operate by transmitting one or more authorizations to a receiver; on a receiver requesting a list of authorized services or authorization for use of a specific service; or, for services such as pay-per-view movies, on a credit scheme, where the credit is transmitted to or provided with the receiver, and said credit is reduced through usage of pay-per-view content. The credit may be based on a financial amount, a number of tokens or other methods that are known to those of skill in the art. Once the CA system has authorized access, the receiver can access, and, if required, decrypt or perform whatever processing is required to allow the receiver to allow user access to the signal.

These CA systems may be compromised in a manner that allows for unauthorized viewing. Methods of compromising these systems include deliberate or accidental operational errors, exploitation of design or operational flaws in the systems, and "hacking" or reverse-engineering of the systems using sophisticated techniques and equipment. Components of the CA system often include a smart card, custom microprocessor or some other sort of microprocessor, hardware, software or storage.

Detection of unauthorized viewing is often rendered difficult, as a compromised receiver may not have a method of communicating back with the operator, or the return communication means may be disabled.

Correction of CA problems is typically a lengthy process, with compromised (also known as "pirated") systems remaining in operation for several years, with a succession of counter-measures and counter-counter-measures being deployed respectively by the distribution system operators and the hackers.

Once a CA system has been compromised, there is typically no separate determination of whether the receiver is making unauthorized usage of content, as the CA system is the only means of controlling access to the content on these receivers.

SUMMARY

In accordance with the present invention, an apparatus and method are provided to identify unauthorized signal usage by identifying signal usage indicia or patterns which are not expected to occur on authorized receivers. Once unauthorized usage is identified, the invention optionally allows for prevention of signal usage.

DRAWINGS—FIGURES

As included within this document.

DETAILED DESCRIPTION—FIGS. 3-14

According to one embodiment of the present invention, there is provided a method and apparatus for detecting unauthorized signal usage in a wireless or wired signal distribution environment. The method of the present invention can determine whether unauthorized usage of signal is taking place even when network and receiver based security systems, as previously described, have permitted access to one or more signals. Once unauthorized viewing is detected, the method of the invention may directly or indirectly hinder or prevent usage of one or more features or signals by the receiver.

Embodiments - Execution environment

In one embodiment of the invention, a method is provided wherein a process operates within the signal receiver, and allows the receiver to make unauthorized usage detection by comparing actual signal usage to permitted usage indicia or patterns. The method can operate even when there is no facility available or operating for the receiver to report usage patterns to the network operator.

The method operates by comparing one or more actual signal usage records with indicia or patterns of legitimate signal usage. These expected patterns may include a check for usage of signals which are not normally authorized in combination to a single user. For a television viewer, examples include a viewer in one city watching local stations from his own city and local stations from another city, a combination which is not normally authorized; a check for the existence of a purchase record when a pay-per-usage signal is being used, such as a television pay-per-view movie; checks for viewing of usages of multiple pay-per-usage signal within a short time frame, as compared to normal pay-per-usage signal viewing, in which, in the television example, a viewer would normally only purchase and view a single pay-per-view program at a time and not purchase multiple programs and switch or "channel-surf" between them; and a check for usage of signals which are never authorized for subscriber usage, which, in the television example, would consist of a channel that is used internally by the network operator or that is created and distributed specifically for the purpose of detecting unauthorized signal usage.

In one embodiment, the method of the invention is implemented as one or more an interactive television (iTV) processes that are transmitted along with a television channel to a satellite television receiver. This embodiment will be referred to as the *iTV embodiment*. A process is transmitted along with one or more television channels. When the viewer selects the channel, the iTV subsystem within the receiver captures and executes the process. The process may be provided in a binary executable format, or as code requiring the services of an interpreter, depending on the particular iTV environment's implementation and capabilities.

The process transmission may be implemented as a separate transmission stream that is associated with one or more channels, as would be implemented, for example, in an OpenTV system, or as a stream of data that is embedded within the video or other component of the signal such as the vertical blanking interval,, as would be implemented, for example, in a WebTV or Wink iTV application, or in a V-CHIP control sequence. The process as transmitted may also consist or a referral or link to another process available within the receiver, within the same or another transmission stream, or from another server available on a network accessible to the receiver. For example, in a WebTV environment, the application transmitted with the video signal may contain an Internet URL that links to a web site of other source of applications or data.

The method according to the embodiments of the invention described herein may be implemented by way of software, hardware or combinations thereof. The method may be implemented in part or in whole within one or more existing hardware or software components within the receiver, on network components, or combinations thereof. These may include, and are not limited to the following.

- As forming part of or using one or more capabilities of the software, hardware or combinations thereof of a receiver. The method of the invention or one or more portions thereof may be included as functionality within the hardware, software or combinations thereof.
- As forming part of or using the capabilities of one or more hardware or software subsystems or combinations thereof of the receiver, such as an electronic program guide, a menu system for selecting content, a targeted advertising system, a measurement and viewing reporting subsystem, a viewing control system such as a V-CHIP parental control subsystem, a copy protection subsystem, or other software or hardware. Subsystems such as these may beactivated when a channel change or other content selection is made by the user, when a change of content occurs on the same system and is indicated by the EPG or by other data transmitted with the content. The methods of may operate as one or more additional functions within one or more of these subsystems.
- As forming part of or using the capabilities of one or more hardware or software subsystems of server components of the network, or a combination of receiver and server components. For example, in a switched signal environment such as a DSL network, all channel change requests are transmitted to network components to effect a change to the signal going to the receiver. As this network component manages the channel change, it has the ability to execute one or more functions of the method of the invention, or to pass data or instructions to another server on the network to execute one or more functions of the method of the invention.
- As forming part of one or more components of a conditional access system used by the receiver. The conditional access system may have hardware or software components within the receiver or on the network that are capable of executing the functions of the method of the invention. Components executing the functions may include hardware or software that are built into the receiver, that are peripheral to the receiver such as a smart card, or that are external to the receiver such as a server for authorization in a switched network environment such as a DSL system.
- As forming part of one or more processes that are transmitted to the receiver as partial updates to one or more software components, as software associated with content, or as software that is used as content, or as software that is used as a function of the receiver. For example, an EPG application may consist of an iTV application that can be sent to a receiver separately from the receiver's main application. The EPG may include one or more steps of the method of the invention, or may in turn include application execution capability that would support a separate application implementing the method of the invention.
- As forming part of one or more of any of the above, and one or more sets of one or more data elements each usable by one or more of any of the above that are transmitted to or otherwise accessible from one or more or any of the above. These data elements may act as parameters to control the operation of the method. For example, data elements transmitted within the EPG data may contain the list of channels on which the method is to be executed, or which components of the method.

The method may be built into the receiver, network components, or combinations thereof, or the receiver, network components or combinations thereof may be updated to contain one or more steps of an embodiment of the invention by a software update, firmware update, hardware or peripheral device update such as a smart card, or combinations thereof. For example, many digital television receivers on satellite networks are equipped to check for software updates being transmitted, and to receive and load these updates. In many such cases, the receiver has the ability to receive software or firmware updates, and the software update being transmitted may include one or more components of the method of invention. Other methods of triggering or effecting a receiver or server software or hardware update are known to those of skill in the art.

Other methods are available for loading software and data on receivers may include:

- repeated transmission of the software, and the receiver periodically checking for the transmission. For example, on many satellite television receivers, turning the receiver off using the remote control or a front panel button puts the receiver in a mode where the receiver monitors satellite transmissions for software and data updates. Messages can also be sent to one or more receivers to switch to the software update detection state
- receiver checking for available updates from one or more network servers. The receiver may do this by communicating with one or more network servers, or broadcasting a request for information on any updates available. This type of request is typically based on a trigger such as a receiver being turned off, turned on, connected to electrical power, or other deliberate or unintentional user-initiated event.

Embodiments – networks and receivers

One embodiment for the invention is a receiver for a television distribution system such as a direct-to-home satellite television environment. Other embodiments for the invention include:

- Television distribution networks, whether wired or wireless, or analog or digital, such as cable television, multichannel multipoint distribution service (MMDS) microwave, terrestrial broadcast, switched networks such as high-speed digital subscriber loop (DSL) and fiber-optic based networks, with receivers for the respective networks or receiving functions built into the television
- Switched and broadcast networks for distribution of other forms of audio, video, data, games, software or other forms of digital content, including cellular telephone networks, gaming networks for video games, digital radio networks, the Internet, and others.
- Receiving devices such as cellular telephones, personal digital assistants (PDAs), personal computers, cable and DSL modems, home entertainment systems, video games consoles, televisions with built-in receivers, audio receivers and other devices. The devices may be designed for real-time playback, for downloading of content for subsequent playback, or for both.

Embodiments – Implementation Detail

In an embodiment of the invention, the method of the present invention as previously described is initiated following a channel change on the receiver. The method or steps of the method may be initiated using other methods as follows:

- Initiating execution following a user-generated trigger event on the receiver. The operating system, iTV subsystem or other software on the receiver may provide facilities to initiate a designated process or instructions following a given user initiated event. These can include channel changes, selection of a channel on the EPG, turning the receiver on or off, selecting the "previous channel" function, or other functions. In many receivers, turning the receiver off does not completely power off the receiver, and functions may be initiated.
- Periodic execution based on a timer triggered by the receiver operating system
- Periodic execution based on a timer triggered by a network component
- A trigger based on a software or hardware interrupt from a receiver operating system or other hardware or software subsystem indicating a state change, which, in the television environment, would be a channel change
- Initiation of the process by another process such as an electronic program guide (EPG), a viewing measurement process or other process

Other methods of initiating a process on a receiver will be apparent to those of skill in the art.

FIGS. 3A-3C show some of the possible distribution of processes of the method of the invention within various embodiments.

FIG. 3A shows an implementation of the method of the invention within a television receiver 16. The receiver contains elements capable of executing a series of functions implemented in hardware, software, or combinations thereof to receive, decode and present television content to the viewer, and to allow the viewer to retrieve the content. In such an implementation, the steps of the method and the data accessed or created by the method may be available from the various subsystems that may be implemented in hardware or software within the receiver, examples of which are described herein. The delivery of processes, data and other elements to the receiver may be dependent on other devices and subsystems available on the network or in the receiver, examples of which are described herein.

FIG. 3B shows an implementation of the method of the invention where the functions of the method are implemented one or more server 80 components which are external to the receiver 16. As an example of such a system, in a switched environment such as the Internet or a DSL system, the receiver requests a particular content stream, which may then be transmitted to the receiver. The acquisition of records and other processes may therefore take place outside of the receiver in the system that receives the channel change requests, or on a system which can receive or access the channel change request data from the server. Other examples where one or more functions of the method are provided in one or more server components are described herein.

FIG. 3C shows an implementation of the method of the invention wherein the functions of the method are distributed between one or more server components and a receiver. A given functions or feature of the method may be located on a single server or receiver, or may be distributed between one or more servers and a receiver. In the embodiment shown in FIG. 3C, the acquisition of usage records take place on the receiver. However, the log of usage records 161 is stored the server 80. The analysis of usage records also takes place on the server. Other features of the method, such as parameter list 180 to direct one or more of the processes of the method, may be present on servers and receivers. The optional preventive

action 300 has elements on both the server component and the receiver component. As an example, on the server, the optional preventive action 300 process may generate a list of parameters or commands for transmission to one or more receivers. On the receiver, the optional preventive action 300 process may receiver the commands or parameters in order to perform the appropriate preventive action. Other examples where one or more functions of the method are provided in one or more of server components and a receiver are described herein.

Further information on the functions and steps of the method and apparatus of the invention and how they may be implemented within receivers and network components are described in the following sections of this document.

Steps of the invention

FIG. 4 illustrates the steps of the method of the invention which occur within one or more processes. The steps are the acquisition of one or more usage records 100, the analysis of the usage records 200, and if the analysis 200 determines that unauthorized signal usage is deemed to have occurred, the optional initiation of preventive action 300 may be undertaken.

Acquisition of usage records 100

The acquisition of usage records 100 is used to acquire one or more records of signal usage. In one embodiment, the record may comprise an identifier for the current content being used on the receiver, which, in the television receiver example, may be the channel number or other code for the channel being viewed.

In an embodiment of the invention which is implemented as a process within a television receiver, the acquisition of usage records 100 is implemented by using a function or access to a memory location or register which returns an identifier for the channel currently being viewed.

Based on the capabilities of the receiver and the functionality available to a process within the receiver, one or more function calls, memory or register accesses, data access or other method of accessing data, or combinations thereof, may used to acquire data for a usage record. The usage record may contain data such as a channel identifier, the date and time of the content usage, information on the content such as the program name, the schedule start time for the program, the time and date of the viewing, the content type for authorization purposes (subscription channel, pay-per-view event, or other characteristic), and other information that is available to the process.

In other embodiments, other methods for acquisition of usage records may be available based on the execution environment and implementation of method of the present invention, and include:

- Passing of the current receiver state as one or more parameters to the acquisition of usage records 100 process as part of the process initiation. This method may be of use when the method is implemented as part of a software subsystem such as an EPG which already has the required information.
- A function call to the operating system or another subsystem within the receiver which can provide access to the records. An EPG subsystem, an iTV environment, a viewing measurement subsystem or a targeted advertising system would typically

have the information and may provide the functions required. Other subsystems may also be capable of providing the functions or data required.

- A memory access to a specific memory or other storage location where the required information is stored
- Where a server external to the receiver receives the channel change request, such as would be the case in a switched environment such as a DSL or Internet–based digital television or other signal delivery system, a process on the server can capture the channel change request or the resulting channel change, or pass the channel change information to another process on the same or another server.
- Periodic polling of the receiver or a server component. A process can execute on a server which requests one or more records from the receiver, or from a server process that has acquired one or more records from the receiver.
- Requesting or accessing of the viewing records from another system or subsystem within the receiver or external to the receiver that is used to maintain viewing records, such as a diagnostic subsystem, an audience measurement system, targeted advertising system, electronic program guide software or other system Such system may accumulate records within the receiver, and may also gather records from the receiver for storage on one or more server systems.
- Data from a subscriber management or conditional access system that holds limited viewing records reported by a receiver. For example, a subscriber management system will collect pay-per-view purchase records from a receiver, either directly or indirectly through a conditional access system.
- Using the data from state information, memory locations, registers or access to functions or features of the receiver operating software or any subsystem that can provide the current state for features of the receiver. Such state information may include information on content the viewer is currently or has recently used. State information may depend on the features available on the receiver and the related data these features may require. Examples of these features include the "previous channel" feature, which, in a television receiver, holds information on the channel that was viewed prior to the current channel being viewed; the picture-in-picture feature, which will have data on two viewed channels; the "previous channel" feature that may be associated with a picture-in-picture feature, and may therefore have data on four separate channels, including the current main picture channel, the previous main picture channel, the current picture in picture channel, and the previous picture in picture channel; the recording function on a PVR-equipped receiver, which may be recording from a channel while a viewer is watching another channel. The data from this feature provides access to another viewing record, and may be available through one or more of the preceding methods.

Other methods of acquiring the viewing records will occur to those of skill in the art.

Figures 5A, 5B and 5C are flow charts showing the steps of acquiring one or more usage records 100. In FIG. 5A, the usage data 111 represents the source of the data. This data may be from one or more of the methods and sources described above, using one or more functions as appropriate for the source of the records. The acquire records 110 step obtains the data from the required source and then places it in records 120 for further use by the other steps of the method. The records 120 may be in the form of variables in memory within the process, in shared storage, in parameters to a function call for the next step of the method, in a record for transmission to another process or system, or other form of storage that would allow access to another process or transmission to another system or process. In some implementations, the records 120 may simply consist of the same data and storage location as the data 111, providing the data 111 is accessible to subsequent steps of the

method as required. The storage of one or more records may involve transmission of the one or more records to another process or system that will in directly or indirectly store the record or portion thereof.

In figure 5B, an optional logging process 140 is used to enter the records 120 into a log 161. The optional logging is detailed below and in figures 6A-6D.

FIG. 5C shows additional detail of the acquire records 110 step. In step 112, the usage data 111 is accessed using one of the mechanisms described above. In optional step 114, additional data may be accessed as required to create the usage data. For example, the viewing data 111 may consist of data from a memory location, register, parameter passed to the process, result from a function call or other method that provides the current channel number. Additional viewing data such as the program type may also be acquired in step 112 from sources such as the EPG. In step 114, other data such as the time of day may be acquired from a memory location, result returned from a function call, memory location, parameter passed to the process or other method. In step 115, one or more usage records 120 are created using the data acquired in steps 112 and 114. The process of creating the usage records 116 may require their creation or availability on another system, in which case the records would consist of one or more data structures for transmission to another software component on another system.

While some embodiments of the invention may require multiple viewing records, the method does not require that all viewing records be obtained or retained. For instance, a periodic polling of the receiver state may not have the records for all the content viewed, but one or more iterations of the process can nevertheless generate sufficient data to make a determination of unauthorized usage.

.Optional logging of usage records

The acquisition of usage records 100 may optionally store one or more of the usage records in one or more logs. One or more elements of the usage record may be stored. The records to be stored, the log in which they are stored, and the elements of the record to be stored may be selected based on the channel or content type, time of day, volume of records, availability of storage space and other factors.

FIGS. 6A-6D show the steps of logging process 140 that may be used in the creation of a log 161, the entry of records into the log 161, and the management of log.

FIG. 6A shows the basic steps for entering a usage record into a record log 161. The test for existence of the log 150 and the log creation160 are optional steps within a logging process 140, as a log may be defined and initialized within a process or apparatus of the method of the invention. For example, the log 161 can take the form of an array that is defined and initialized as a set of one or more memory storage variables or records within the program that implements the logging process.

Where the log does not exist, the create log 160 step may allocate the storage space required and may initialize the space as required to allow storage, retrieval and management of the records.

The log 161 may be represented as a set of records stored in memory, on disk, or in any other form of storage accessible by the processes of the invention. The log may take the form of one or more records, which may consist of a sequential list of data, a set of records,

a file or other storage format. The physical storage may be in any form of storage such as memory, registers, or disk or other forms of storage, and may be located on or accessible to any of the systems or subsystems described within the embodiments or execution environments. Even volatile forms of memory may be in an embodiment, as long-term storage of the records may not be required, as the method may not require a complete or extensive set of records. The log 161 may be in a form that provides a measure of self management, such as a circular log, where any new entry overwrites the least recently used entry. The log may also be in a form that requires management, in which case filtering and log management processes may be required as described below.

In one embodiment, the log 161 can use a small amount of storage by keeping a single bit for each channel that is of interest for unauthorized signal usage detection purposes. A bit value of zero would indicate that the channel had not been used, and the bit for a given channel would be set to one when a usage record indicates that the channel has been used.

The step of adding one or more records to the log 170 takes one or more viewing records 120 and enters them into the log 161. The method of updating will depend on the format of the log selected. If the log 161 takes the form of a record of whether or not a given channel is viewed, then the entry to the log would simply update the existing record for the particular channel. If the log 161 is intended to gather both channel information and the time of viewing, then a new record may be appended to the log. The acquisition of usage records may also transmit log records to a separate network component for storage and further processing as described in the methods and embodiments herein..

FIG. 6B is a flow diagram of logging process 140 with the additional optional steps of filtering the log entry 165 and managing the log 190. The optional filter log entry 165 process may be used to reduce the number of entries in the log based on conditions stored within the process, or using parameters available to the process. For example, logging may only be required for specific channels, and therefore some entries may be deleted and not logged. The list of channels to be logged may be stored as data within the process, or may be provided as data in a parameter list 180 that is accessible to the process.

Record filtering may include elimination of consecutive records for the same service or content (example: in a periodic polling scenario, consecutive records for the same channel may be deleted since there is in effect no state change from the first record); limiting the storage of records to signals of interest to the operator from a theft of signal perspective; limiting the records to a single record per channel or instance of content, and other mechanisms. Where a single record is kept per channel or instance of content, an existing record may be updated with the current record. For example, if only a single record per channel is kept and the record includes the time the usage occurred, the time of usage could be updated with the time from subsequent viewing records for the same channel. A variety of compression methods can be used and are known to those of skill in the art.

The optional manage log 190 process is used to further manage the content, size, location or other features of the log.

A logging process may use encryption, checksums, digital signatures and other techniques to protect the content of the log from being accessed or tampered by other processes or hackers attempting to circumvent the method of the invention. Furthermore, information which may be unique and may be available from a subsystem within the receiver or other source accessible to the logging or other processes may be used to make the storage identifier, location, encryption key or other characteristic of the log unique to one or more

receivers, or to change the location or other characteristics of the log on a periodic basis, thus increasing the difficulty for a person or persons attempting to determine the means of operation of the method of the invention. A logging process may modify, move, delete or replace the existing log structures. In this manner, means that may be used by hackers to detect, disrupt, or destroy the log structures can be circumvented. In such cases, the create log 160, add log record(s) 170 and manage log 190 may require access to parameters 180 or other data to coordinate the placement, method of entry, access and management of the log entries.

In other embodiments, the logging, log creation and log management functions may be within the same process or occur as separate processes. The logging and log management functions would only execute if the log had already been created by an instance of the log creation process. FIG, 6C shows a flow for a separate process that is used for log filtering and management. The filter log 166 process, in this case, may filter based on the current content of the log and not on the record currently being written. The process of figure 6C may be dependent on the prior execution of a process that creates the log. FIG. 6D shows a separate process that creates a log.

Other methods of log management will be apparent to those of skill in the art.

Analysis of usage records

The analysis of usage records 200 performs analysis on one or more usage records to determine if unauthorized usage has occurred. Several tests and comparisons may form the analysis of usage records 200 as described in the following methods.

METHOD 1 – Usage of unauthorized combination of signals and indicia

FIGS. 7A and 7B are flows diagram of embodiments of the analysis of signals used 200 that verifies that one or more content usage records available from the acquisition of usage records 100 are not present in combinations of records or in combination with other indicia that would not be expected through normally permitted use or authorization of the receiver.

Examples of inconsistencies of usage of channels include the viewing of local stations from multiple communities on satellite television systems such as the DISH Network from EchoStar Communications Corporation, Littleton, CO, and DirecTV, from Hughes Electronics Corporation, El Segundo, CA. These operators carry the local stations from multiple US cities. A viewer's receiver should only be authorized for the local signals for the local city or area which the viewer has registered a subscription with the operator. Another example includes the viewing of cable and satellite television channels that are only authorized for viewing in certain geographical areas, such as the regional signals from Fox SportsNet from Fox Entertainment Group, New York, NY. In Canada, premium signals like, for example, The Movie Network from Astral Media Inc., Montreal, Canada, may only be normally authorized for subscribers in the eastern part of the country, and signals for Movie Central from Corus Entertainment, Inc., Calgary, Canada, may only be normally authorized for subscribers in the western part of the country. Unlike legitimate system users, users of a compromised system may be able to view such combinations of signals that are not normally authorized for subscribers in a single area.

The use of such signals can be used to make a determination of unauthorized viewing. Without knowing the location of a receiver, the use of a first signal normally authorized only for a first geographical area and a second signal normally authorized for a second

geographical area that does not overlap with the first geographical area indicates the tviewer is not authorized for one or both of the signals.

In optional step 210 of FIG. 7, parameters can be retrieved to configure the operation of the method. Data and data structures can be used to generalize the algorithms and processes. For example, a list of channels that are incompatible with a given channel number may be available in memory that is part of the process, or in memory or data that are accessible to the process. Test may be limited to a limited number of records or record combinations. For example, in a given execution instance of the method, the comparison may be limited to a predetermined number of the available records.

In step 211. a record is retrieved from the available records. Typically, the analysis may start with the most recent record. The record may come from any of the record storage structures created or populated by the acquisition of records. The figure shows both the viewing records 120 from the most recent acquisition of records, and the usage record log 160. However, in typical operation, only one or the other may be used. The process of getting a record will depend on the storage structure used for the usage record, and may be as simple as accessing a memory location or register.

In step 212, the usage record is checked against other usage records or indicia to determine if unauthorized usage has occurred.

In one embodiment, an iTV process associated with one or more specific channel checks to see if other incompatible channels are included in the available viewing records. For example, such a process could be associated with all local stations from the Atlanta market, and check for viewing of local stations from other markets.

The test for a list of incompatible signals for a given signal may be implemented in several ways in various embodiments of the invention. The following pseudocode samples are examples of some the possibilities.

- Coding within the process of specific tests against one or more sets of one or more channels. In one embodiment, the process implementing the test is associated with one or more channels which are incompatible with another set of channels. For example, if a given set of channels are never authorized with channels 201, 202, 205, 206, 207 and 208, then the following set of instructions would provide detection of unauthorized usage for a program associated with said given set of channels:

```
for all records available
        if record.channel=201
        or if record.channel = 202
        or if record.channel >= 205 and record.channel <= 208
                then unauthorized_usage = true
        next record
end for
```

- Checking against combinations for multiple channels or content instances. For example, if channel 201 is never authorized with channels 203 or 204, and channel 300 is never authorized with channel 301, the following process could be run on the receiver for any channel of content access:

```
first_record = get_record()          /* get the first record */
```

```
while more records available
        next_record=get_record()      /* get the next record */
        if first.record.channel= 201 and
                (next.record.channel=203 or next_record.channel=204)
        then unauthorized_usage
        if first_record.channel=300 and next_record.channel=301
        then unauthorized_usage = true
end while
```

In embodiments where the optional logging is not used, the tests can occur against the limited set of records available to the process. For example, in an embodiment where only the current and previous channels are available, the steps of processes 100 and 200 of FIG. 3 could be implemented as follows:

```
/* Step 100 */
current_channel=get_current_channel()
prev_channel= get_prev_channel()
/* Step 200 */
if (current_channel = 201 and (prev_channel=203 or prev_channel=204)
or (current_channel=300 and prev_channel=301)
then unauthorized_usage = true
```

Where the process is attached to one or more specific channels with a common set of incompatible channels, the process can be further simplified. In the previous example of channel incompatibilities, channel 201 is incompatible with channels 203 and 204. The following process could be associated with channel 204:

```
/* Step 100 */
prev_channel=get_prev_channel()
/* Step 200 */
if prev_channel=201
        then unauthorized_usage = true
```

Other embodiments determining if channels are compatible include the use of one or more structures such as arrays or matrices. Such structures could be stored within the process executable; as data structures, files or other storage or transmission mechanisms accessible to the processes as optional parameters 180 acquired in step 210. In the iTV embodiment, for example, the processes and data files containing the list of incompatible channels could be transmitted within the iTV streams. As an example of such a data structure, a matrix is provided as a file that is transmitted within an iTV stream that is accessible to an iTV process. In one example of such a structure, one index of the matrix may be an individual channel identifier, or a range or set of channel identifiers, and the other index of the matrix is the set of incompatible channel identifiers, ranges or sets of channel identifiers. Other methods for comparing whether two channels are compatible will occur to those of skill in the art. Various techniques can be used to reduce the number or rows and columns in the bit map by only representing rows and columns for channels that are to be tested for compatibility.

In another embodiment, use of one or more signals intended for a given geographical area can be compared against one or more indicia that may be used to derive the intended location of the receiver to make a determination of unauthorized usage. For example, data

pertaining to the time zone in which a receiver is intended to operate, or a current time can be used as an indicator of geographical location for the receiver. A receiver that has an indicator for Eastern Time zone and that is watching a channel that is normally only authorized for a western time zone is operating in an unauthorized manner. Other examples of indicia that may be available in a receiver to indicate its intended location include location codes such as a US Postal Service ZIP code; one or more blackout zone indicators as typically used to control viewing areas of sporting events; and other data that may be sent specifically to a receiver to indicate location.

In such an embodiment, the get next record step 211 and the test for all records processed in FIG. 7 may be omitted if only the currently used signal is to be tested against one or more indicia.. The test for inconsistent channel usage would test a record against a value or range of one or more indicia. For example, if the viewing record is for a local channel from Los Angeles, the test could check if a ZIP code stored in within the range of ZIP code values for which local Los Angeles stations may be provided.

In other embodiments, the location of the receiver may be determined by other locating means including global positioning system (GPS) subsystems and other systems as may be known to those of skill in the art.

In another embodiment, one or more indicia may be sent to one or more receivers or to systems or subsystems within or accessible to an embodiment of the method described herein. Such indicia can be created primarily for other purposes or specifically for the purposes of an embodiment of the invention. For example, in the iTV embodiment, for a high-value service such as a premium movie channel, one or more iTV programs can be created and transmitted to store a data element on one or more receivers. Within the application, different values for the data element can be set based on whether a receiver is authorized or not to receive the premium channel. Such a program can be applicable to a range of receivers, and can set the variable on each receiver within the range or receivers to indicate whether or not the receiver is authorized to receive the service. The same mechanisms described earlier for controlling access to logs and other data on the receiver may be applied to the storage and retrieval of such data elements. Once one or more such data elements have been created and set on the receiver, a separate process can test for the existence of one or more such data elements or for values of such data elements against available usage records to determine if the presence or value of one or more data elements is consistent with the values of one or more usage records. For example, a process may create a specific variable, bit string, file or other data element only on receivers in a list of one or more receivers. The same process or another subsequently running process can check available usage records for indication that a specific channel was viewed, and, if so, can then check if an appropriate data element is present and has a specific value to indicate that the specific channel has been authorized.

Blackout control systems are typically only used for specific sporting events based on sports franchise broadcast rights. In one embodiment of the invention, the blackout system is now used to control use of an entire channel based solely on the intended geographic area for r the signal, and not on specific sporting events. The blackout system may be used directly to control unauthorized usage for stations only authorized in specific areas. A blackout definition may be negative, in which the geographic area defined for the blackout is not authorized to receive the signal governed by the blackout, or positive, in which only the area defined for the blackout is authorized to receive the signal.

METHOD 2 – Usage of pay-per-usage signal without purchase r cord

FIG. 8 is a flow diagram of an embodiment of the analysis of signals used 200 that verifies if a pay-per-usage signal has been properly purchased. In the preferred embodiment, pay-per-usage signals consist of pay-per-view movies, events or other programs.

In many television receivers within as known to those in this art, the purchase of a pay-per-view signal through usage of receiver functions may result in the creation of an event purchase record within the receiver. The pay per view purchase may also be reported from the receiver to a server such as a conditional access system, a subscriber management system, other systems, or combinations thereof, by way one or more of the communication networks available to the receiver. The user of the receiver may have functions available on the receiver that allow the user to review which pay-per-view signals or other content was purchased using the pay-per-view or other credit-based functions.

In a receiver where the security has been compromised, a user may be able to access or view pay-per-view content and signals without first going through the pay-per-view process. Therefore, in cases where a security has been compromised, there may not a purchase record where one would be expected when a viewer is accessing pay-per-view content. The viewing of the signal is initiated with a simple channel change and without going through the purchase process, and therefore no purchase record is created.

In one embodiment, the process containing the steps of FIG. 8 is executed against a set of one or more records of pay-per-view channel viewing. Step 230 retrieves the PPV purchase records, which may be available from a receiver or a network component. The PPV records 181 may be directly accessible to the process through memory, file or other storage access; through a function call, network protocol or other form of request of communication with a subsystem such as the RCAS system on the receiver that may have the information, or through access to another component. Step 231 compares the one or more PPV viewing records with the PPV purchase records available to determine if purchases were made for one or more of the PPV records. If at least one PPV viewing record does not have a corresponding PPV purchase record, then unauthorized usage is determined to have occurred.

The comparison of the purchase records and the current usage records of step 231 could potentially require more than just the channel number, as multiple pay-per-view events can be scheduled on the same channel, and certain events on pay-per-view channel may not be pay-per-view events. The comparison may in such cases be made against an event identifier code or against the time and date of the event. Other data items and methods for matching usage records to purchase records will occur to those of skill in the art.

In another embodiment, a process such as, for example, an iTV process, can be provided specifically for a given pay-per-view event. in another embodiment, step110 can be omitted and the comparison of step 231 will look for a specific data value in the purchase log.

The comparison of purchase records to signal usage records in the purchase record for signal used test 231 can compare the purchase records to one or more of the available usage records. The number of records used for comparison may be limited using criteria such as a maximum number of records, the records from a given period of time, the records from a set of channels, or other criteria. Such limitations may be based on usage parameters. Such parameters may be made available by including the optional step 210 of method 1 to acquire the appropriate parameters, and implementing the test 231 in a manner

that uses the parameters. Such limitations and methods for setting the limitations may be applicable to the other methods for determining unauthorized usage described herein.

The other steps in FIG. 8 are as described for the prior figures.

METHOD 3 – Concurrent usage of multiple pay-per-usage signals

FIG. 9 is a flow diagram of an embodiment of the analysis of signals used 200 that verifies if multiple pay-per-usage signals have been used within a pre-determined time period.

A pay-per-view signal typically has a purchase cost associated with its usage, and the user must agree to pay this cost as part of the pay-per-view purchase process.. Because of this cost, a television viewer is unlikely to purchase multiple pay-per-view events which are shown at the same time. The viewer is therefore unlikely to switch or "channel surf" between multiple pay-per-view programs or channels. When a receiver's security system is compromised, the viewer may be able to watch multiple pay-per-view channels without accepting or paying the charges associated with the pay-per-view programs. The viewer's behavior may therefore change, as the viewer may now "channel surf" between pay-per-view channels and other channels. "Channel surfing" between pay-per-view channels may therefore be used as an indication of unauthorized usage.

This method identifies unauthorized usage by identifying "channel surfing" between pay-per-view channels as near-simultaneous use of two or more pay-per-view signals. The determination of near-simultaneous use can be made through different means. In one embodiment, viewing records are logged with the time of viewing. Unauthorized usage may be determined if the viewing records show that two or more pay-per-view signal usage records within a pre-determined period of time. In another embodiment, the method uses two or more records from the current state of the receiver, such as the current channel, the previous channel, a picture-in-picture channel, a previous channel for picture-in-picture, or a channel being recorded within a PVR device. If two or more of these records are for pay-per-view signal usage, then unauthorized usage may be determined to have occurred.

In FIG. 9, usage records are compared to determine if they indicate near-simultaneous use of pf multiple pay-per view signals. In one embodiment, the usage records 120 would only represent the current and previous channel used, as implemented on television receivers in the "previous channel" function. No check for a pre-determined amount of time between the two events. If the current and previous channels are determined to be pay-per-view events that require a separate purchase, the test can be considered to indicate unauthorized signal usage.

In another embodiment, the viewing records from either the usage records 120 or a usage log 161 have been stored with a time stamp. The test of step 241 consists of determining whether two or more pay-per-view channels were viewed within a pre-determined period of time. The period of time for the test can be controlled by a parameter X which indicates a number of time units, and the number of uses of pay-per-view content that is used to indicate unauthorized usage within the X time units can be controlled by a parameter Y, where Y is typically set to two or higher.

The test of step 241 may potentially require more than just the channel number for each viewing record, as multiple pay-per-view events can be scheduled on the same channel, and certain events on pay-per-view channels may not be pay-per-view events. The comparison may require a check that the program is a pay-per-view program, that the

program has a cost associated with it, that the program has an identifier or other information to indicate that the program is a pay-per-view event. In some cases, an operator may create free pay-per-view events, which have all the characteristics of a normal pay per view event, but a price of 0, or free. In such cases, the free event would not be considered a pay-per-view event for the purpose of the test. 241. Where the network operator controls the number and frequency of free pay-per-view events, the test of step 241 may not require a test for free pay-per-view events. For example, in the operator ensures that that is never more than one free pay-per-view event playing at any one time, then in the example of FIG. 6B, Y can be set to 3.

The other steps in FIG. 9 are as described for the prior figures.

METHOD 4 – Trap channel

FIG. 10 is a flow diagram of an embodiment of the analysis of signals used 200 that verifies if a channel that is not normally authorized for subscribers has been used.

A network operator may operate signals that are not normally authorized for customer receivers. Such signals may include test signals, signals for internal operations, signals specifically transmitted to help in the detection of unauthorized usage, and other signals. Any usage of these signals can be considered an indication of unauthorized usage. As used within this specification, these various forms of signals are termed "trap channels".

In step 251 of FIG. 10, a usage record is compared against a list of one or more trap channels. If the current channel is a trap channel, then unauthorized usage has occurred.

The other steps in FIG. 10 are as described for the prior figures.

In another embodiment, no test is required. Use of the trap channel itself is sufficient to make a determination of unauthorized usage. A process can therefore proceed directly to a determination of unauthorized usage and take the optional step of preventive action 300., as shown in FIG. 11.

In another embodiment, a trap channel can be created using audio, video or other signals that may be associated with other channels. The trap channel is created with these signals but with separate control information so that the trap service is not available to normally authorized subscribers, even though the same audio and video signals may be part of other services that may be part of normal subscriber authorizations. For example, in FIG. 14, Channel 3 is a channel that may be authorized using normal subscription commands. The same video and audio components are also used by Channel 4. However, Channel 4 has a separate CA stream CA4, and an iTV component iTV2 associated with it. iTV2 contains the software and data necessary to perform a trap function.. Channel 4 is never authorized within a normal subscription. Therefore, only users of compromised receivers would be capable of accessing Channel 4. The conditional access system may provide the control information and data required to generate stream CA4. The multiplexer may provide the encryption and a portion or all of the SI generation facilities, which define the channels and their associated streams.

In FIG. 14, an iTV process such as the process of FIG. 11 may be associated with Channel 4 by being distributed within iTV stream ITV2. The process would therefore only execute for viewers of Channel 4.

Implementation and Operation

The steps of FIG.4 are not required to operate in direct sequence. To minimize use of system resources, one or more processes implementing each of, combinations of or parts of the acquisition of records 100, the analysis of records 200, and the optional steps of preventive action 300, and creation, making of entries to and managing one or more usage logs may occur as a direct sequence as shown in FIG. 4, or may execute independently at different times. However, to successfully execute the method of the invention, a step may require that one or more of preceding steps have executed at least once.
This ability to execute steps of the method independently of the other steps and at different times may provide an embodiment of the invention with several advantages. As performance, space for executable code and data, availability of bandwidth for transmission and other factors may affect the ability of a network operator to distribute applications and data to receivers, network servers or combinations thereof, the ability to send processes implementing only specific steps of the method at any given time may allow the operator to implement an embodiment of the invention on a network or on receivers or on combinations thereof that may otherwise be unable to support a process incorporating all the steps of the method of the invention.

For example, an operator may send a process to create the log structures during the morning. The operator may then send the acquisition of records 100 process during prime time. The following day, the operator may send the analysis of records 200 process to analyze the records captured the previous day, with a preventive action process 300 that, if unauthorized usage is determined to have occurred, sets a flag in the receiver. At a later time such as, for example, the following day, a preventive action process that tests for the presence of the flag and disables the receiver, as show in FIG. 12.

Multiple versions of the processes may be used and transmitted separately. For instance, for a given time period, or for a given set of channels, an analysis of records 200 process that only implements Method 1 may be sent. For another set of channels, during a different time period, an analysis of records process 200 that implements Method 2 and Method 3 may be sent.

This ability to separate the method into multiple sub-processes, and for potentially only certain steps of the method to exist on the receiver at a given time, may provide further advantages. The ability of hackers to determine the nature of the measures being taken to detect and prevent unauthorized usage and to prevent the operation of the method may be made more challenging by intermittent presence of various components of the method within the receiver. As an example, in an iTV environment, a given process that is transmitted with a channel may be replaced by another process when the viewer selects another channel. The ability of the operator to modify and adapt the processes such as iTV processes specifically to counter measures that may be employed by hackers is greatly enhanced, as such a process may not require the rigorous testing of, for example, an operating system or other software component of a receiver.

FIG. 12 is a flow diagram for taking preventive action, where acquisition of usage records 100 and analysis of usage 200 were executed previously, but without taking preventive action when unauthorized signal usage was detected.

Step 260 of FIG. 12 tests to see if a flag has been set to indicate unauthorized use of signal. If such a flag has been set, then preventive action 300 is initiated. A process implementing the steps of FIG. 11 or FIG. 12 may be associated with one or more channels. These

channels may or may not be those for which unauthorized usage was detected. In this manner, preventive action such as disabling of viewing capability can be taken on any or all channels, regardless of whether the channel viewing being disabled has been authorized or has been detected to have been previously viewed on an authorized or unauthorized basis for that user, and independently of the time at which the unauthorized usage detection took place.

Separation in time and in delivery and execution of execution of logging, analysis, preventive action and other functions provides the benefit of making it more difficult to establish countermeasures to defeat the method of this invention, as the various steps can operate at spaced apart intervals, such that an observer seeking to discern the method of the present invention may not be capable of determining clear cause and effect behavior. The optional preventive action 300 step may take different forms, and may affect different services at different times for the time and service on which the user is determined to have made unauthorized usage, making it difficult for the unauthorized user to discern the pattern of behavior that caused the preventive action to be taken. Furthermore, the timing and selection of channels used by different viewers may cause the timing of preventive action 300 and the channels on which preventive action 300 is undertaken to vary from user to user.

In embodiments described above, one or more processes implementing one or more steps of the methods described herein may be transmitted to the receiver as iTV processes that accompany the various television signals, or may be otherwise associated through the EPG or other process with the use or selection of one or more television signals. The processes transmitted may be associated with one or more signals, and different processes may be associated with different types of signals. For example, in an iTV environment, a process implementing a method described earlier for detecting unauthorized PPV usage may only be associated with PPV channels, and another process implementing a detection usage of unauthorized combinations of signals may only be transmitted with geographically-restricted signals.

As an example, in one embodiment shown in FIG. 14, in a DVB-based digital television distribution environment, the television video signal is distributed in one bit stream, the audio in another, and iTV processes in another. A single iTV process stream can be associated with multiple channels within the same transport signal bandwidth. In this example, processes from iTV stream iTV1 may be associated with streams audio1 and video 1 to create Channel 1, and with streams audio 2 and video 2 to create Channel 2.

Optional Preventive Action Process

If the analysis of usage records 200 shows that an improper combination of signal usage has occurred, then optionally a preventive action 300 process may be initiated.

The preventive action 300 may be implemented as one or more processes or steps. For example, upon detection of unauthorized usage, an instance of the preventive action process 300 may simply set a flag to indicate that unauthorized usage has occurred. Another instance of a preventive action process 300 can be execute at a later time, in which the process checks for the flag indicating unauthorized viewing has occurred, and then takes further steps to prevent or otherwise disrupt usage of the receiver.

Other embodiments for the take preventive action 300 process include any or all of the following actions:

- Displaying a message, graphic or other content in a manner that blocks the usage of the underlying content. As an example, when implemented on a television receiver, a message box could be displayed that covers the entire screen.
- Distorting or otherwise hindering the presentation of the content
- Logging a record of the unauthorized usage event
- Switching the receiver to another signal, such as a different channel
- Disabling one or more capabilities of the receiver, or the entire receiver
- Displaying a message to the receiver user
- Reporting the unauthorized usage event to another network component or system using any of the networks or communications protocols that may be available
- Reporting the unauthorized usage event to a conditional access system component within, peripheral to, or external to the receiver
- Testing to verify that two or more instances of unauthorized usage have occurred before one or more actions are taken. A test may also require that the multiple records indicate that the events took part within a given time period.
- Where the preventive action 300 process takes place outside of a receiver, sending flags, processes, instructions or other data to the receiver to prevent usage of any or all signals on the receiver.

Other preventive measures will occur to those of skill in the art, and will be available based on the receiver and network type.

Instances of the preventive action 300 and the actions taken therein may vary from method to method, between channels and services, at different times of day, or based on parameters accessible to the process. In one embodiment, separate preventive action processes for separate methods may set separate flags to indicate that unauthorized usage has occurred, as shown FIG Z.A and Z.B. A given flag may be based on one or more methods, instances, channels or other characteristics.

These flags may be used set on a global basis for the receiver, to indicate one or more forms or instances of unauthorized usage; on a per service basis, to indicate unauthorized use of a single service; or on a class of service basis, to indicate unauthorized use of a group of services such as, for example, the pay-per-view services. A given flag may be a binary indicator of whether the flag has been set, or may contain one or more fields such as a count of the number of times the flag was set to indicate the number of instances of unauthorized usage detection of the type applicable to the given flag, date and time information, and other date.

In some embodiments there may multiple implementations or versions of the preventive action 300 process. These different versions of the process may perform different actions, and may be dependent on prior execution of one or more specific instances and versions of preventive action processes. For example, one preventive action process to disable a receiver may require that flags be set to show more than one type or instance of unauthorized usage has been detected, such as viewing a combination of channels that is not authorized as described in method 1, and channel surfing through multiple PPV channels as describe in method 3. Such a preventive action process will therefore not disable the receiver until other preventive action processes have been invoked to set appropriate flags that indicate the two types of unauthorized usage have occurred. Different

preventive actions may therefore be invoked based on different combinations, types and frequencies of unauthorized usage.

The types of structures that can be used to represent flags are the same as those that can be used to represent records and log entries, as described above. When a flag is first used, a process may check for the existence of the flag, and if it is not available, create the appropriate structures as required.

The same mechanisms described above for controlling access to logs and other data on the receiver may be applied to the creation, storage and retrieval of data elements of these flags.

Embodiments – multiple tests, conditional tests.

FIG. 13 shows how embodiments of the present invention may be combined within a single set of processes transmitted of the receiver, and tests to determine the appropriate method based on the channel type. Tests for additional channel types can be included. As shown in FIG. 13 for pay-per-view channel types, one or more test methods can be applied for a given channel type. For other channels, no method may be required.

The processes may be configurable through the use of parameters to determine the timing, channels, content or other constraints on when the steps of one or more methods as described herein can be executed.

Conclusion, Ramifications and Scope

Although the present invention has been described in terms of various embodiments, it is not intended that the invention be limited to these embodiments. Modifications within the spirit of the invention will be apparent to those of skill in the art. For example, usage of a signal may be initiated by processes or systems internal or external to the receiver, such as personal video recorder (PVR) device or process, a computer, or other component designed to select, record or transmit content on behalf of the user.

The compromising of security on digital television systems is typically limited to attacks on the conditional access system. Compromised receivers will often continue to receive core software and operating system updates, iTV processes, electronic program guide updates and other software. The present invention can in such circumstances therefore be implemented on receivers that have already been compromised to reduce and control unauthorized signal usage.

ABSTRACT

In accordance with the present invention, an apparatus and method are provided to identify unauthorized signal usage by identifying signal usage indicia or patterns which are not expected to occur on authorized receivers. Once unauthorized usage is identified, the invention optionally allows for prevention of signal usage.

CLAIMS

1. A method for detecting unauthorized signal usage in a content delivery network, comprising the steps of:
   a. acquiring at least one usage record for a signal
   b. comparing at least one record to a predetermined signal usage indicator, and
   c. based on the comparison of step (b.), determining whether the said usage record is associated with unauthorized signal usage

2. The method of claim 1, wherein the comparison of usage records consists of a check for usage of combinations of signals that are not normally authorized on the same receiver

3. The method of claim 1, wherein the comparison of usage records consists of a check for the existence of a purchase record when the signal usage record is a pay-per-use signal

4. The method of claim 1, wherein the comparison of usage records consists of a check for concurrent use of multiple pay-per-use signals

5. The method of claim 1, wherein the comparison of usage records consists of a check for usage of a signal that is not normally authorized for receivers

6. The method of claim 1, wherein preventive action is taken to disable at least one capability of the receiver

7. The method of claim 1, wherein at least one process of the invention is transmitted and executed using the facilities of an interactive television system

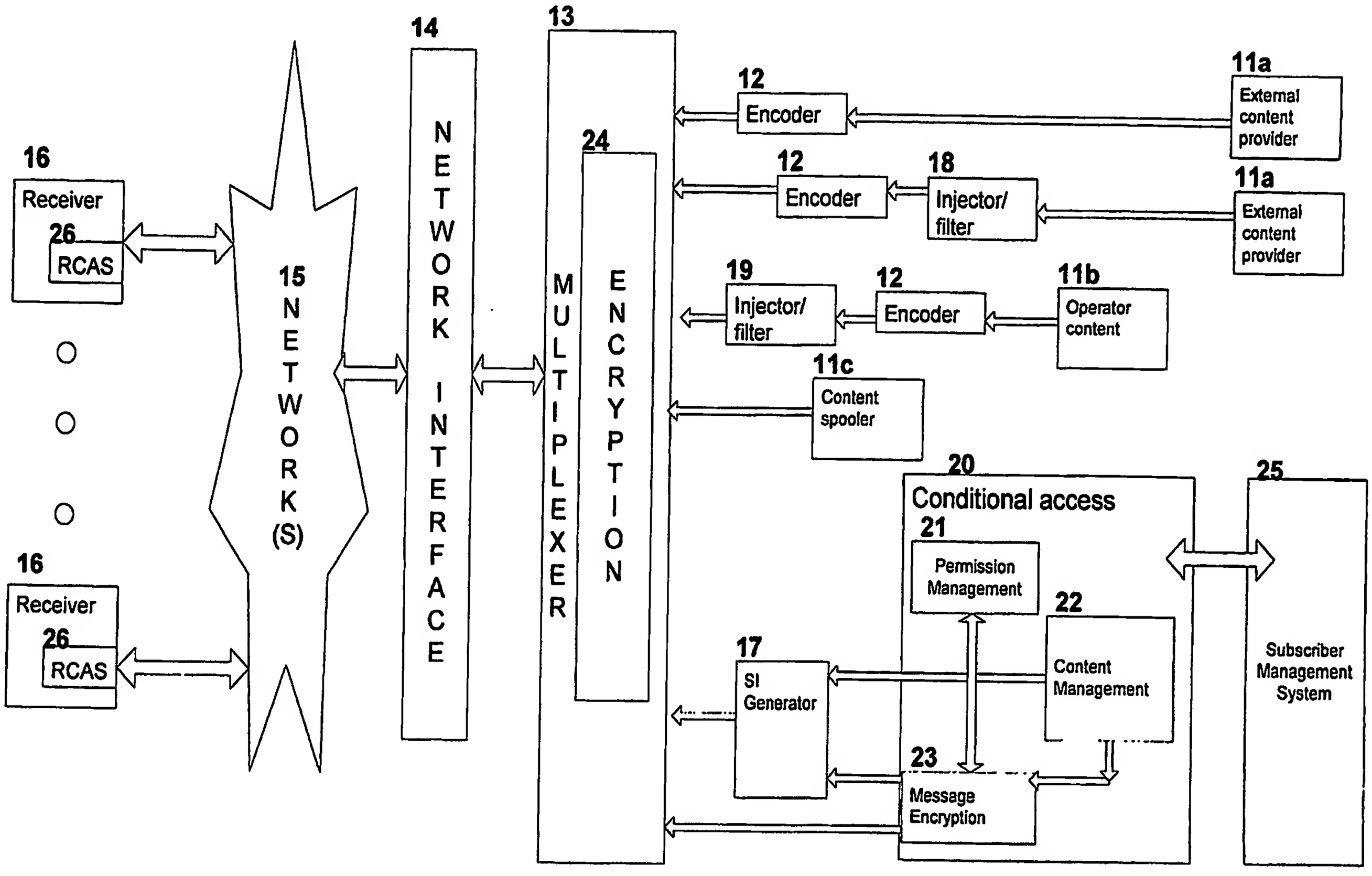
8. The method of claim 1, wherein said comparing at least one record to a predetermined signal usage indicator is performed within the facilities of an iTV process,

9. The method of claim 1, wherein one or more data or processing facilities of the invention are based within a targeted advertising system, a multiplexer, a conditional access system or component thereof, a multiplexer, a blackout control subsystem, or a parental control system.

ADDITIONAL MAIN CLAIMS

10. A method for detecting unauthorized signal usage, comprising the steps of:
    a. associating a process with a specific signal indicative
    a. executing said process whenever the signal is used

Figure 1 Network System 10



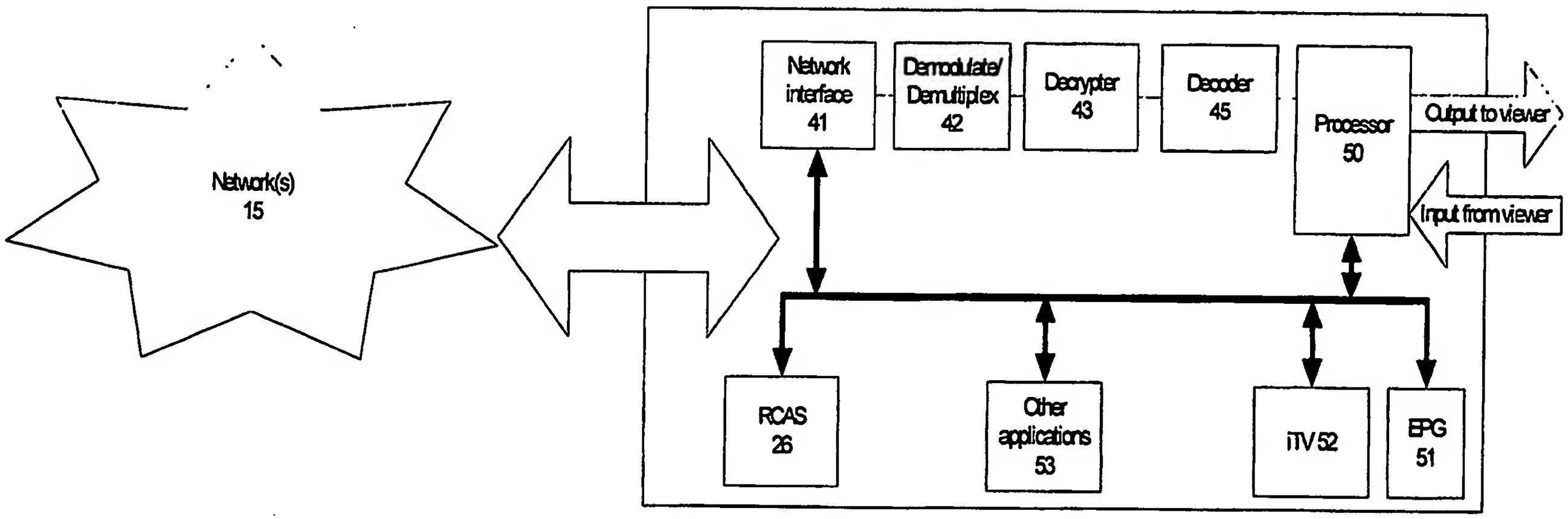

Network(s)
15
Network interface 41
Demodulate/ Demultiplex 42
Decrypter 43
Decoder 45
Processor 50
Output to viewer
Input from viewer
RCAS 26
Other applications 53
iTV 52
EPG 51

Fig. 2

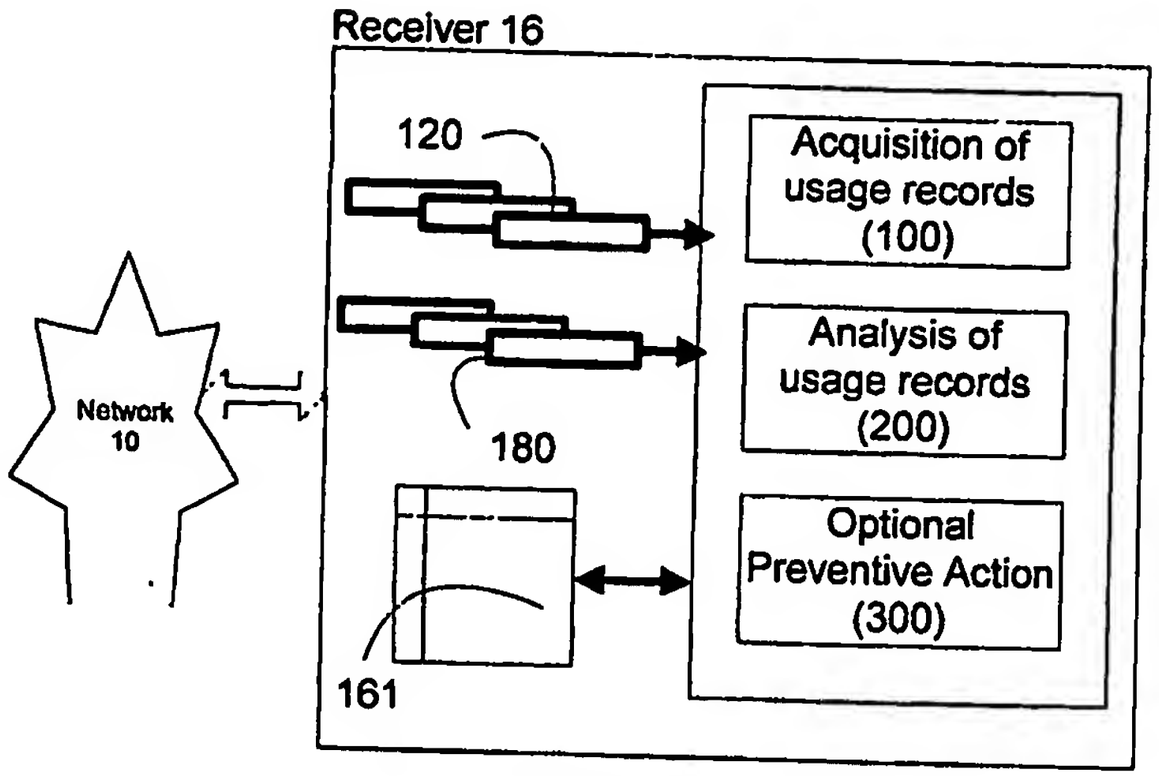


Fig. 3A

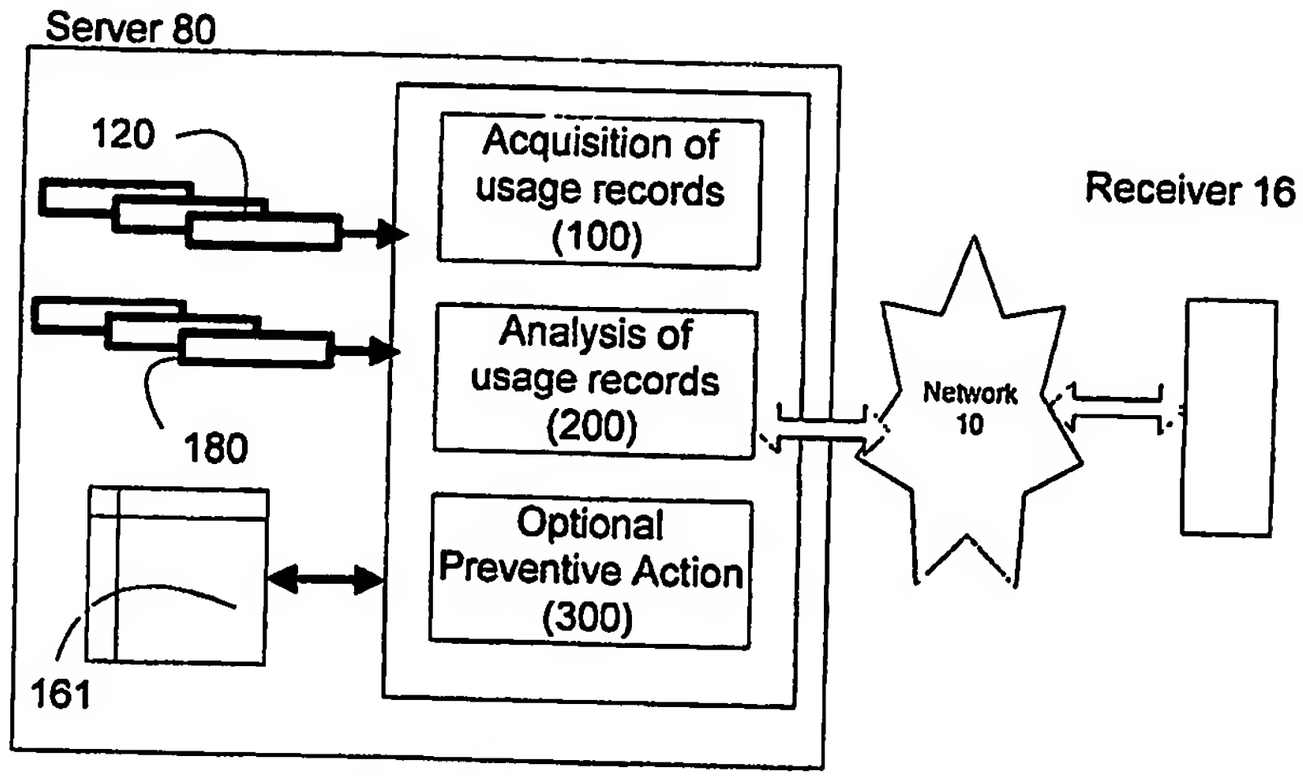


Fig. 3B

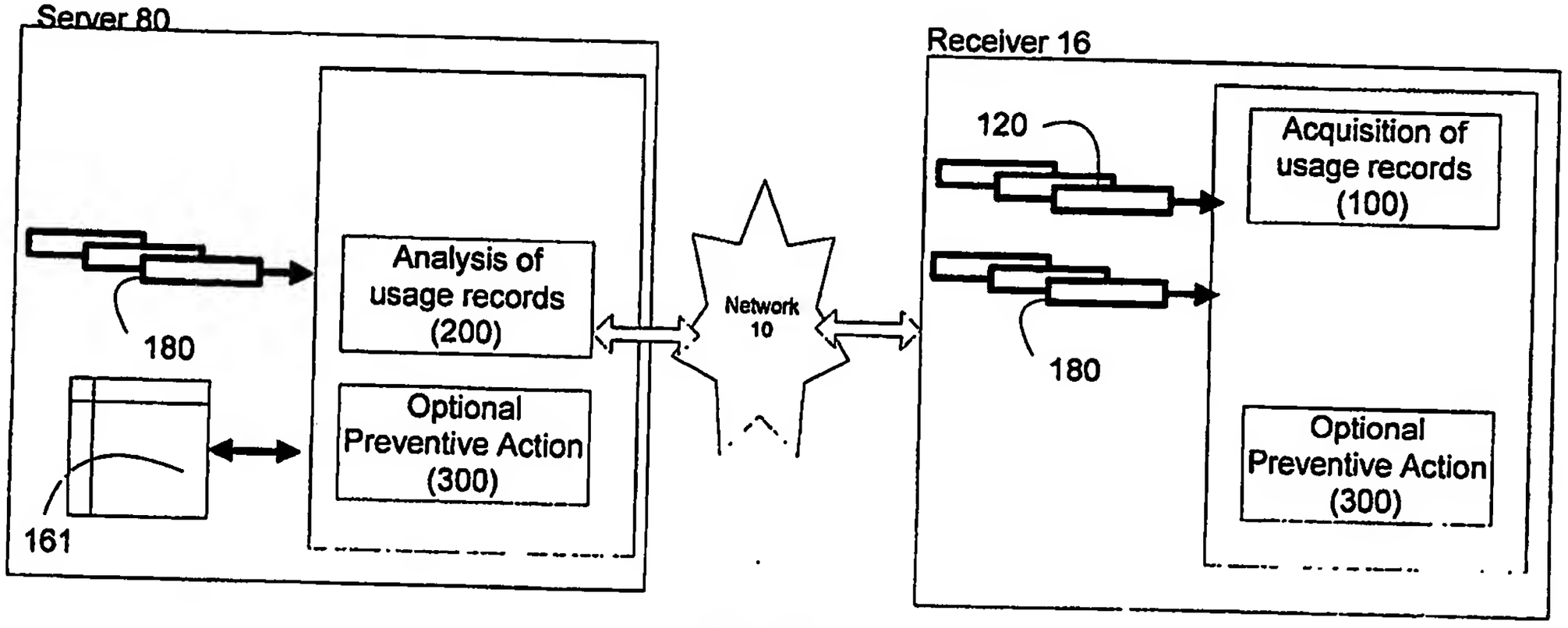


Fig. 3C

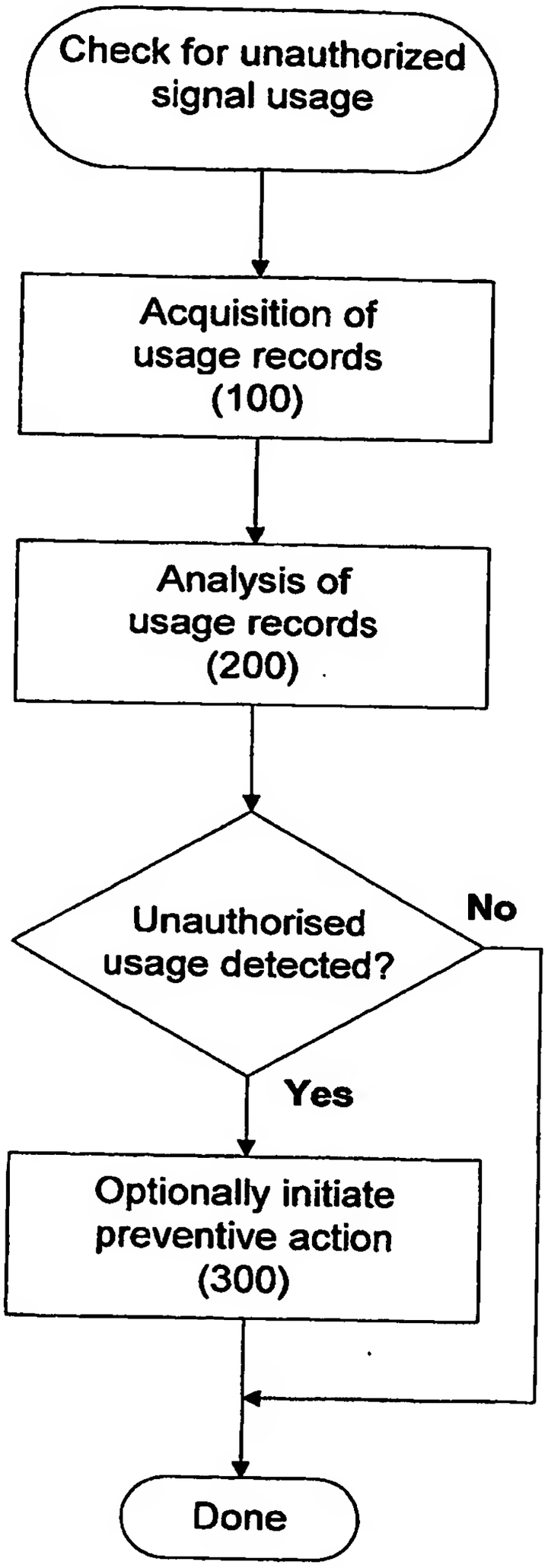

Check for unauthorized signal usage
Acquisition of usage records (100)
Analysis of usage records (200)
Unauthorised usage detected?
No
Yes
Optionally initiate preventive action (300)
Done

Fig. 4

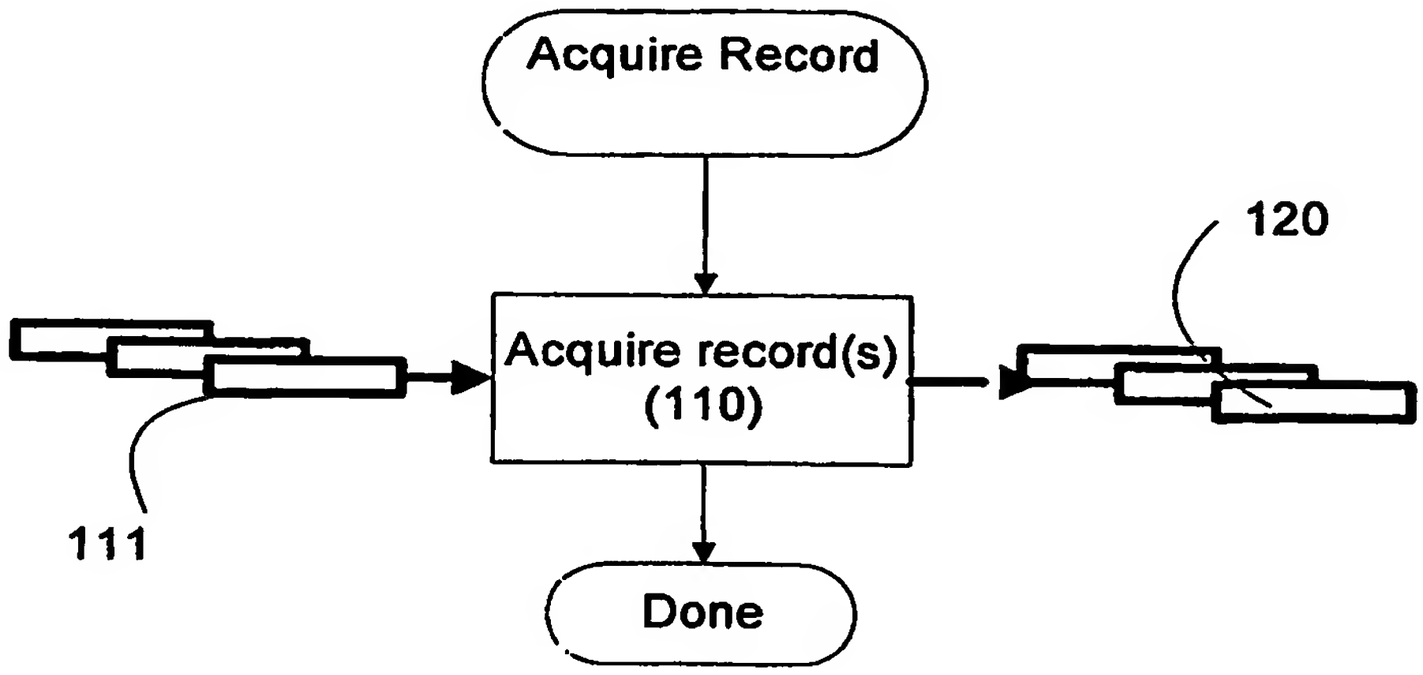

Acquire Record
Acquire record(s)
(110)
120
111
Done

Fig. 5A

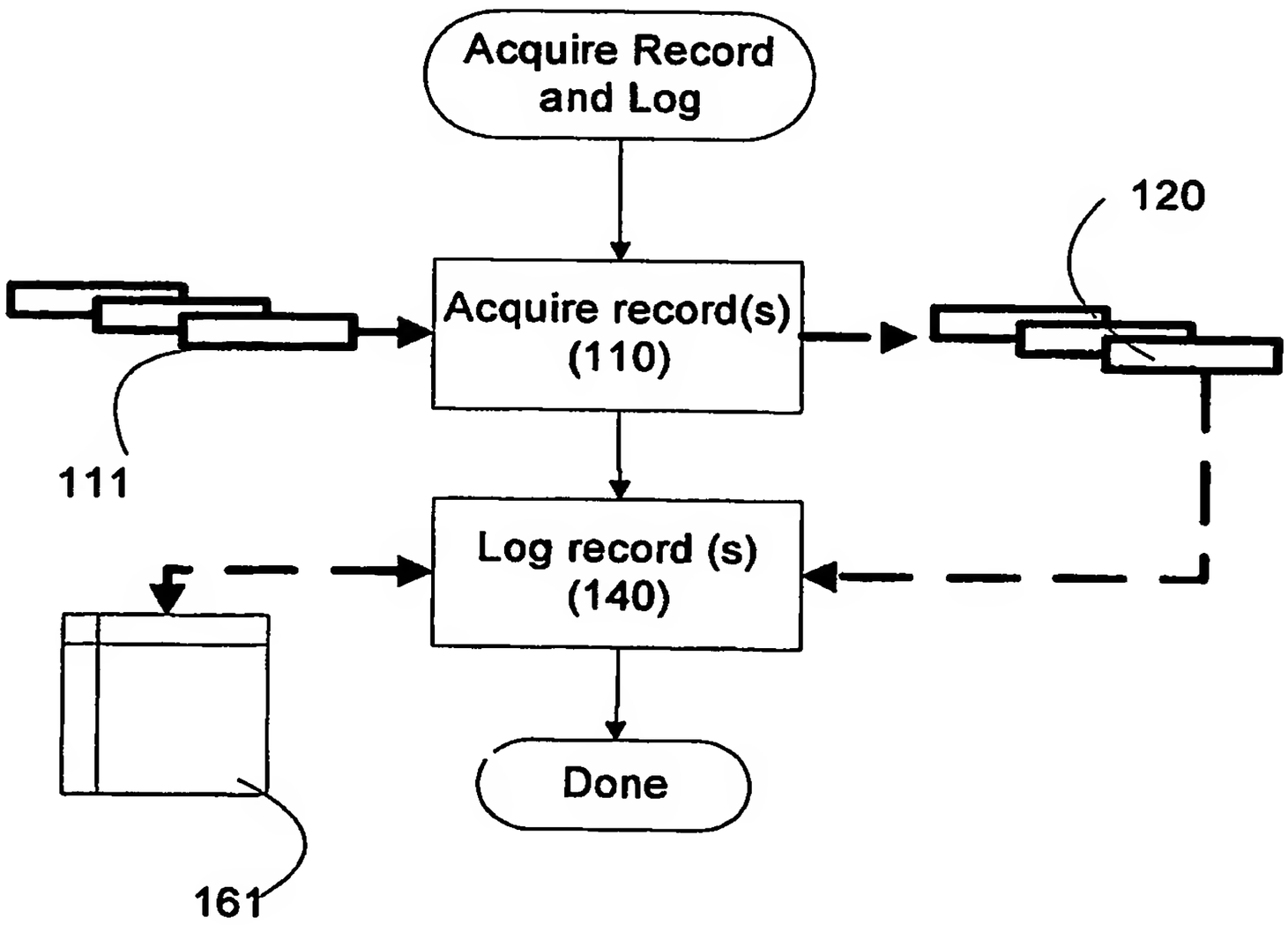

Acquire Record
and Log
Acquire record(s)
(110)
120
111
Log record (s)
(140)
Done
161

Fig. 5B

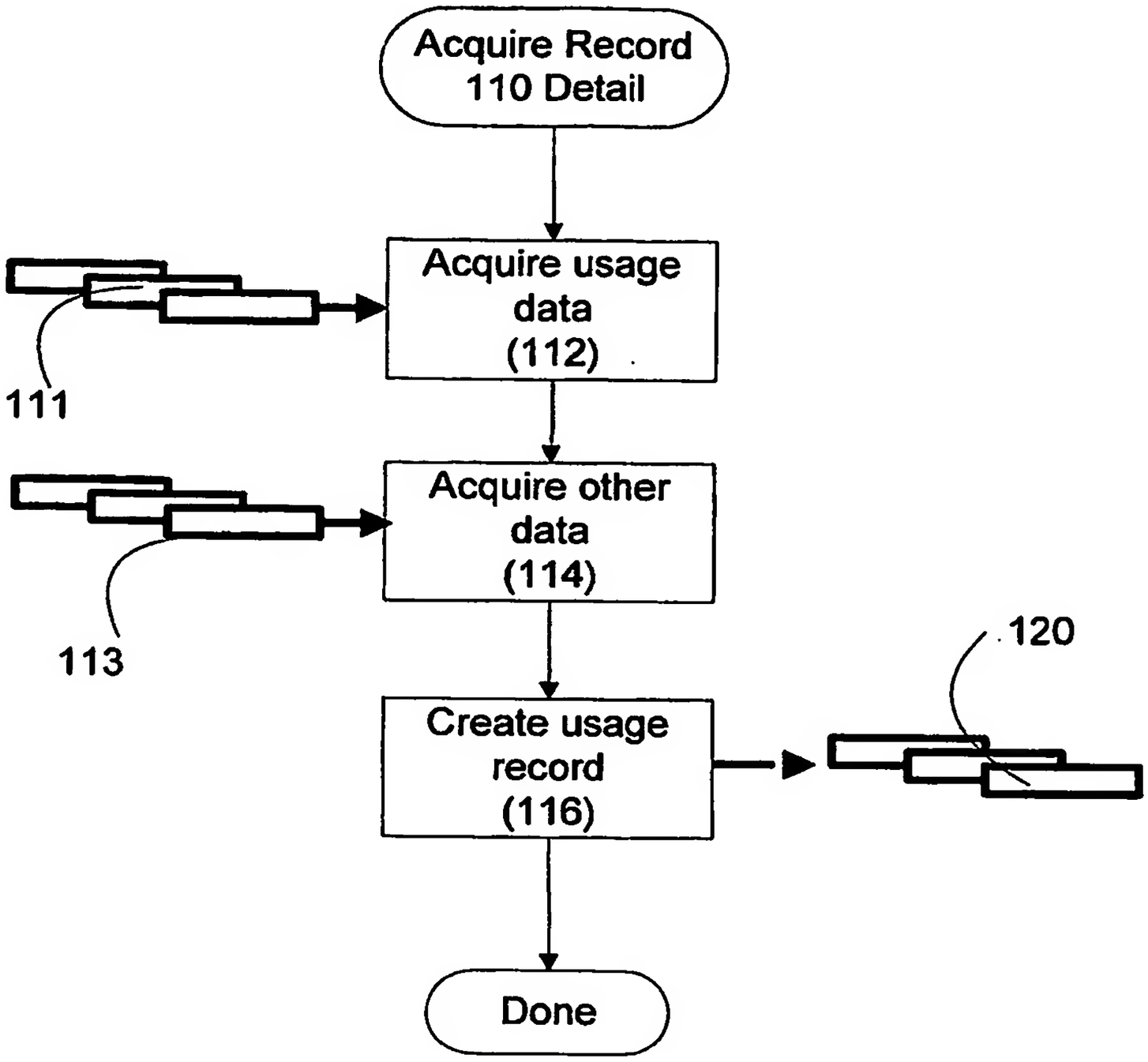

Acquire Record 110 Detail
Acquire usage data (112)
111
Acquire other data (114)
113
120
Create usage record (116)
Done

Fig. 5C

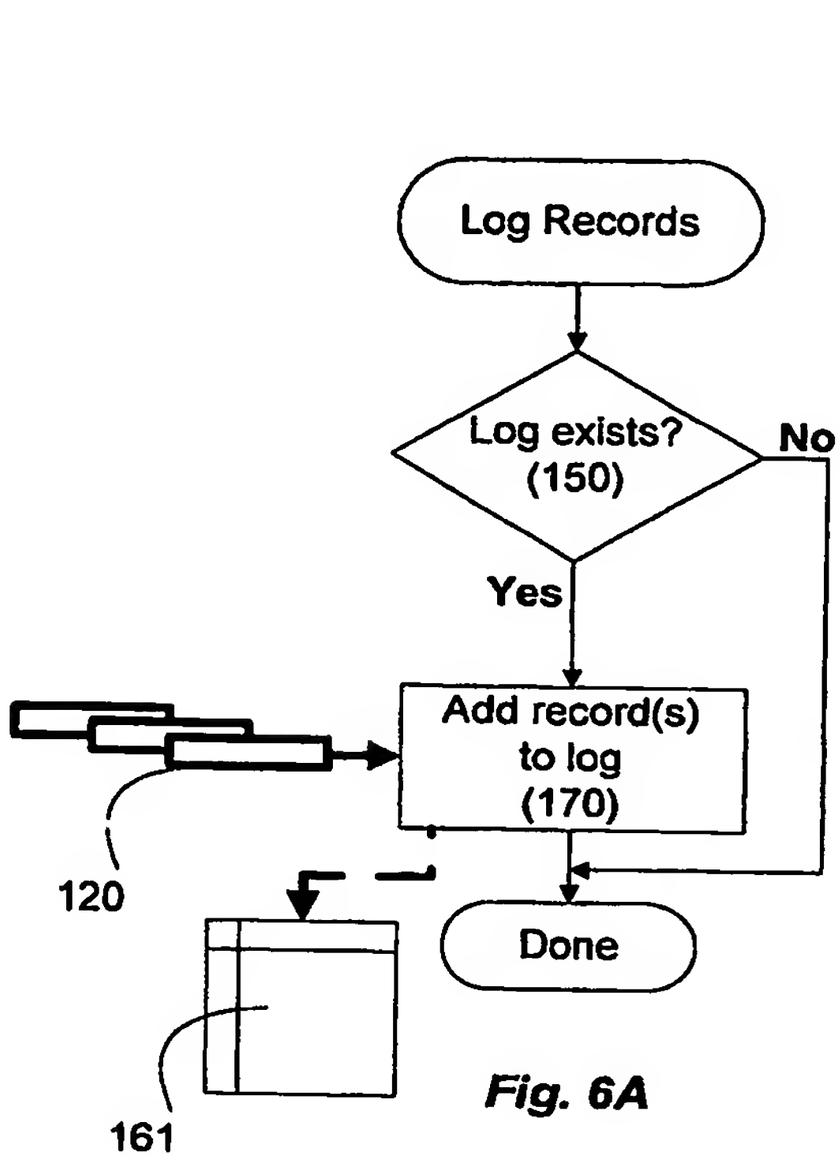


Fig. 6A

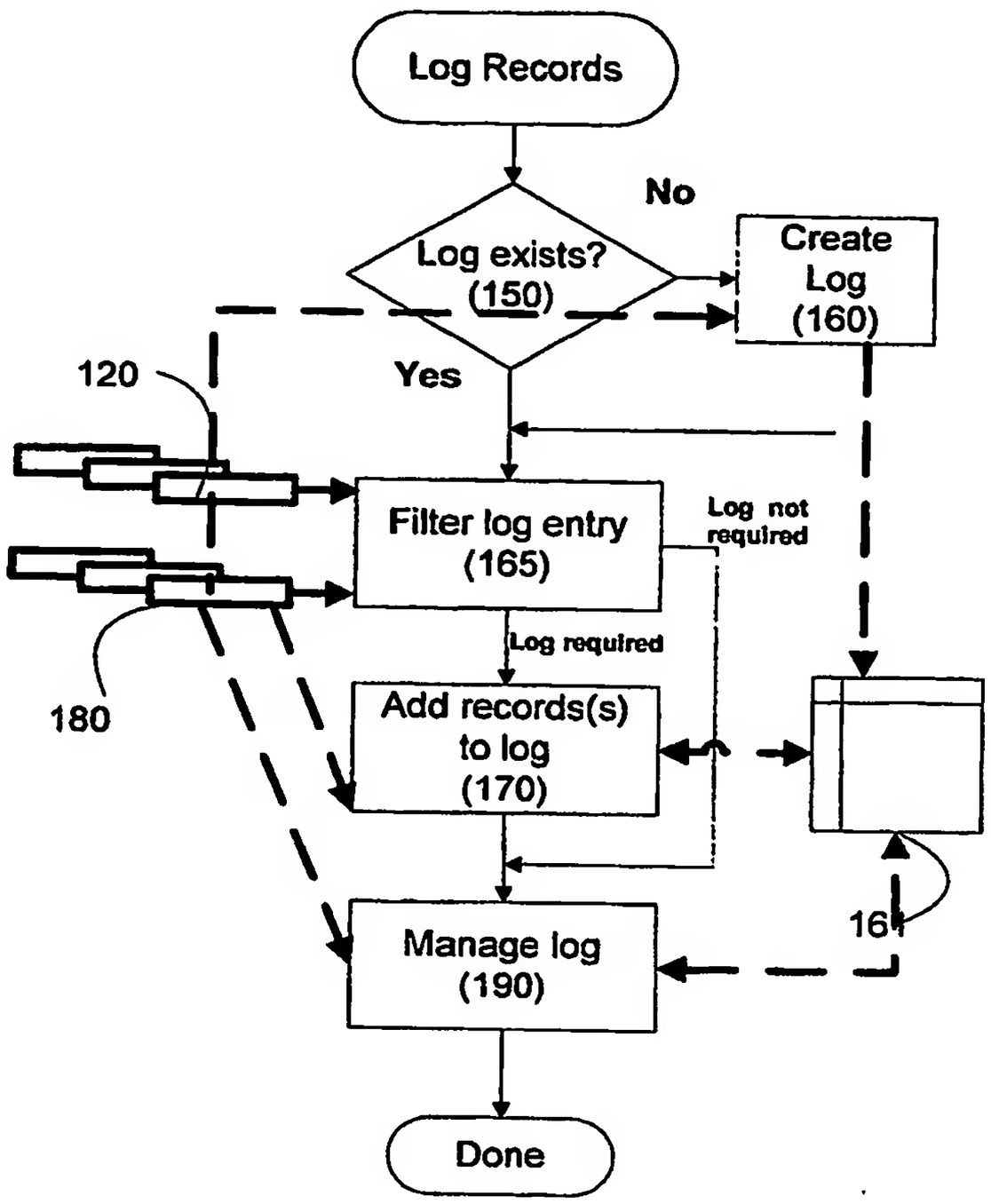


Fig. 6B

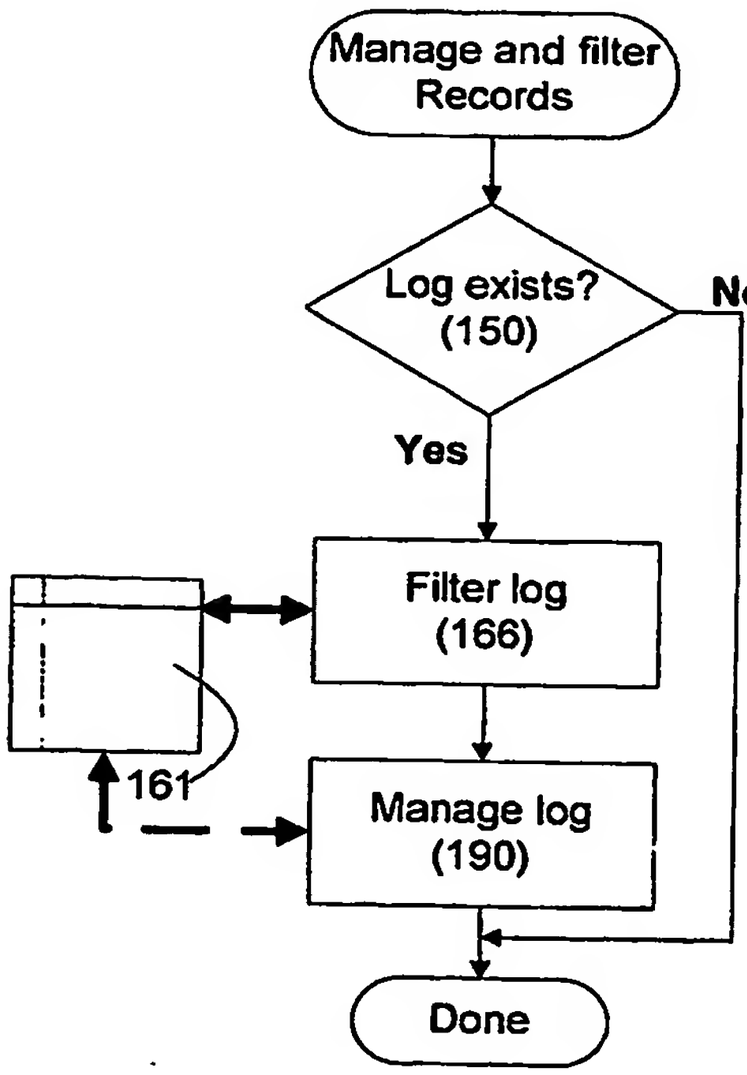


Fig. 6C

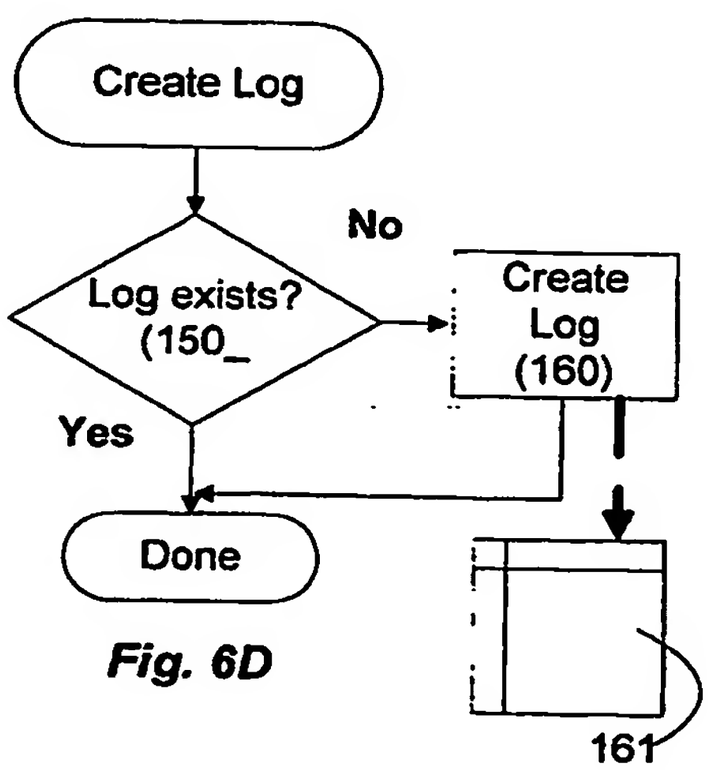


Fig. 6D

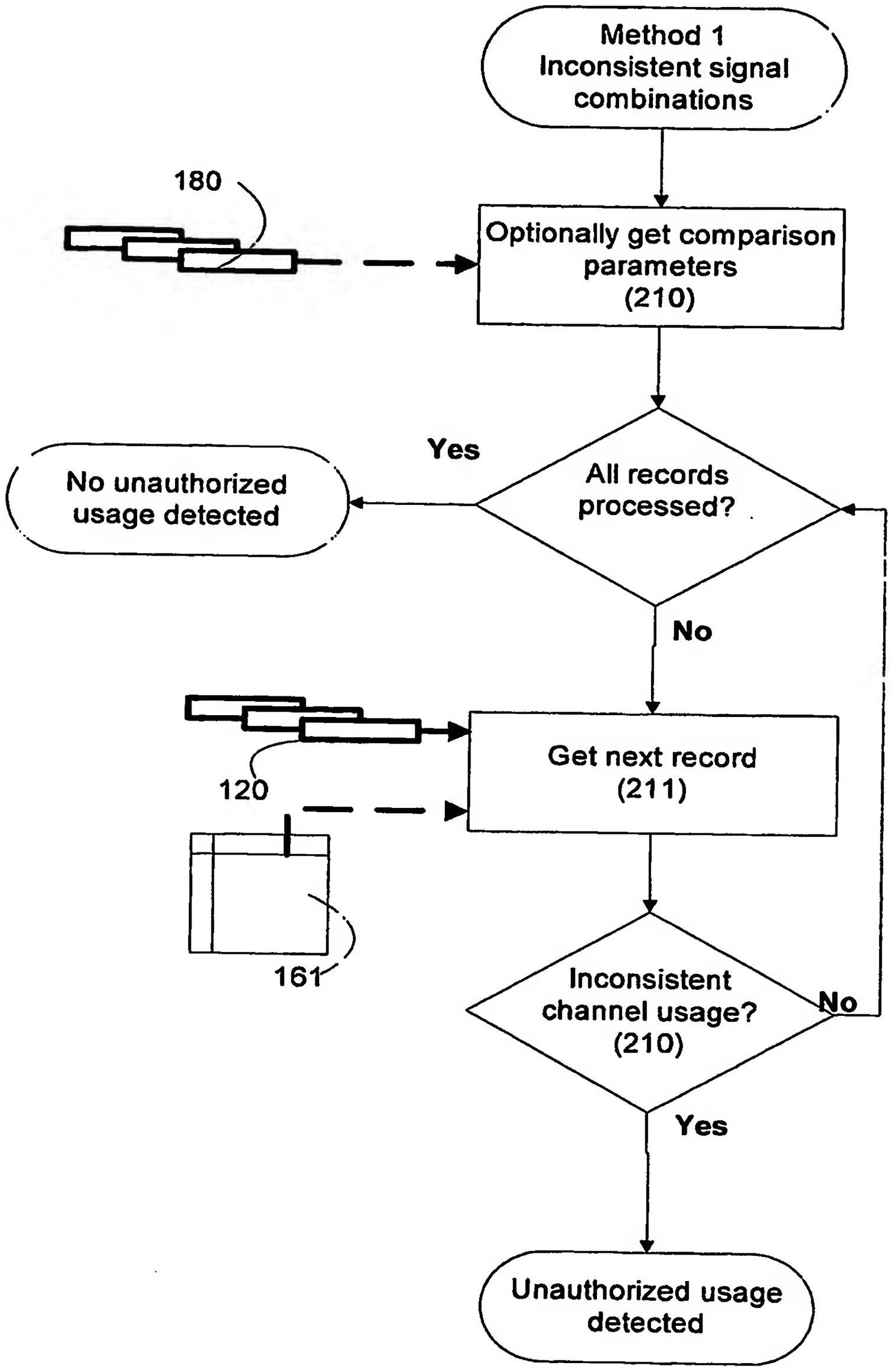

Method 1
Inconsistent signal combinations
180
Optionally get comparison parameters (210)
All records processed?
Yes
No unauthorized usage detected
No
120
Get next record (211)
161
Inconsistent channel usage? (210)
No
Yes
Unauthorized usage detected

Fig. 7

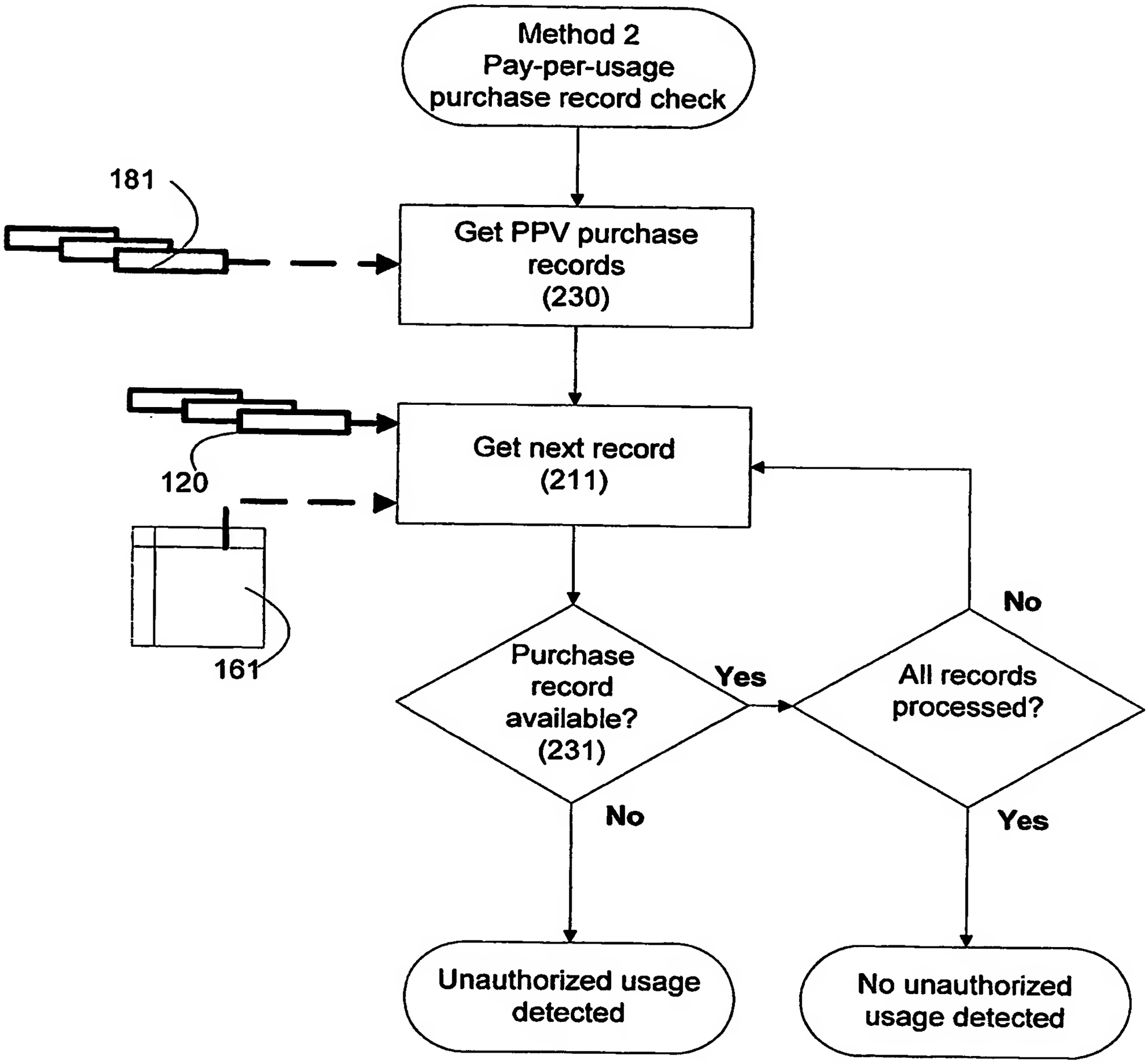

Method 2
Pay-per-usage
purchase record check
181
Get PPV purchase
records
(230)
120
Get next record
(211)
161
Purchase
record
available?
(231)
Yes
No
All records
processed?
No
Yes
Unauthorized usage
detected
No unauthorized
usage detected

Fig. 8

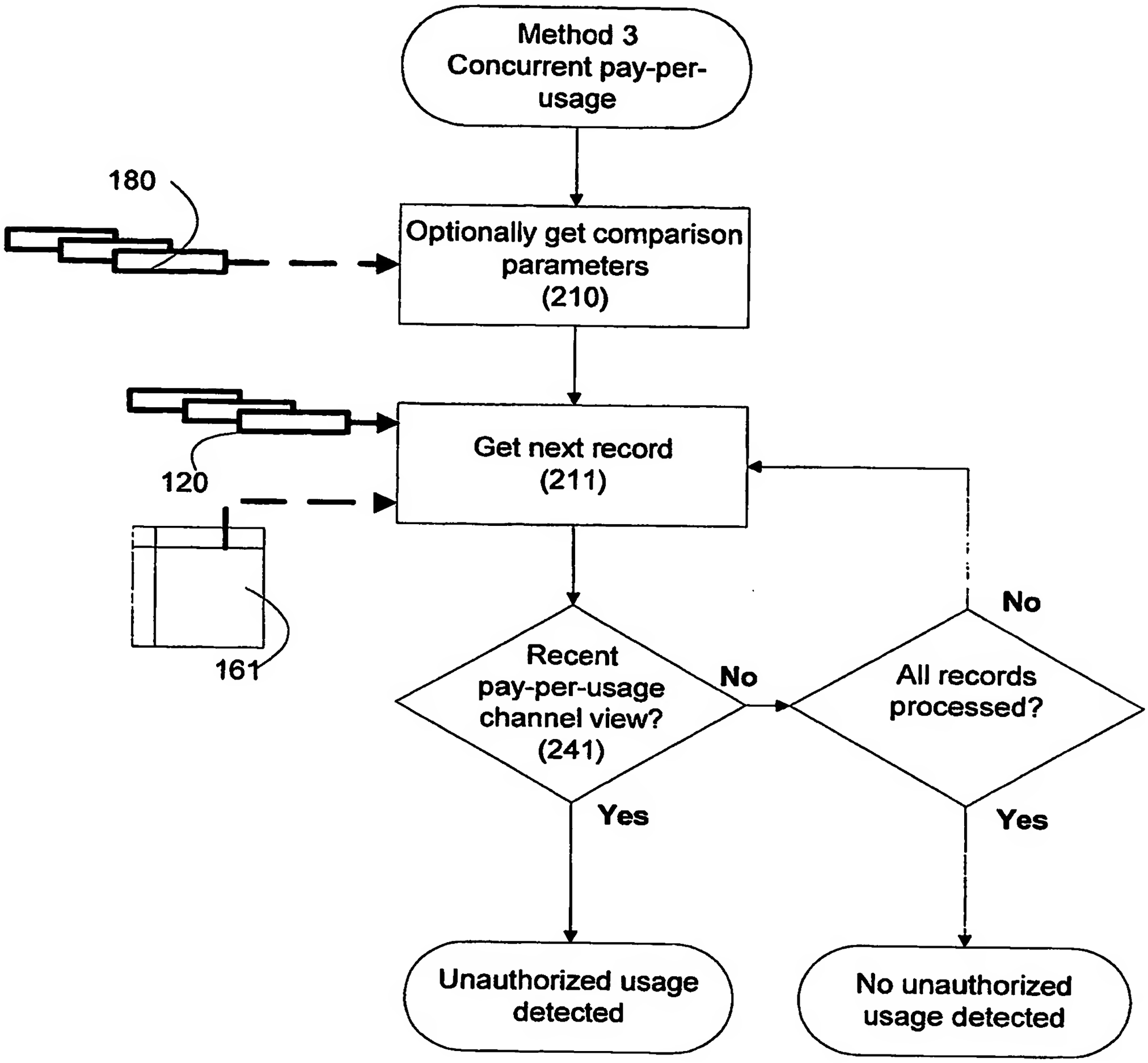

Method 3
Concurrent pay-per-usage
180
Optionally get comparison parameters
(210)
120
Get next record
(211)
161
Recent pay-per-usage channel view?
(241)
No
All records processed?
No
Yes
Yes
Unauthorized usage detected
No unauthorized usage detected

Fig. 9

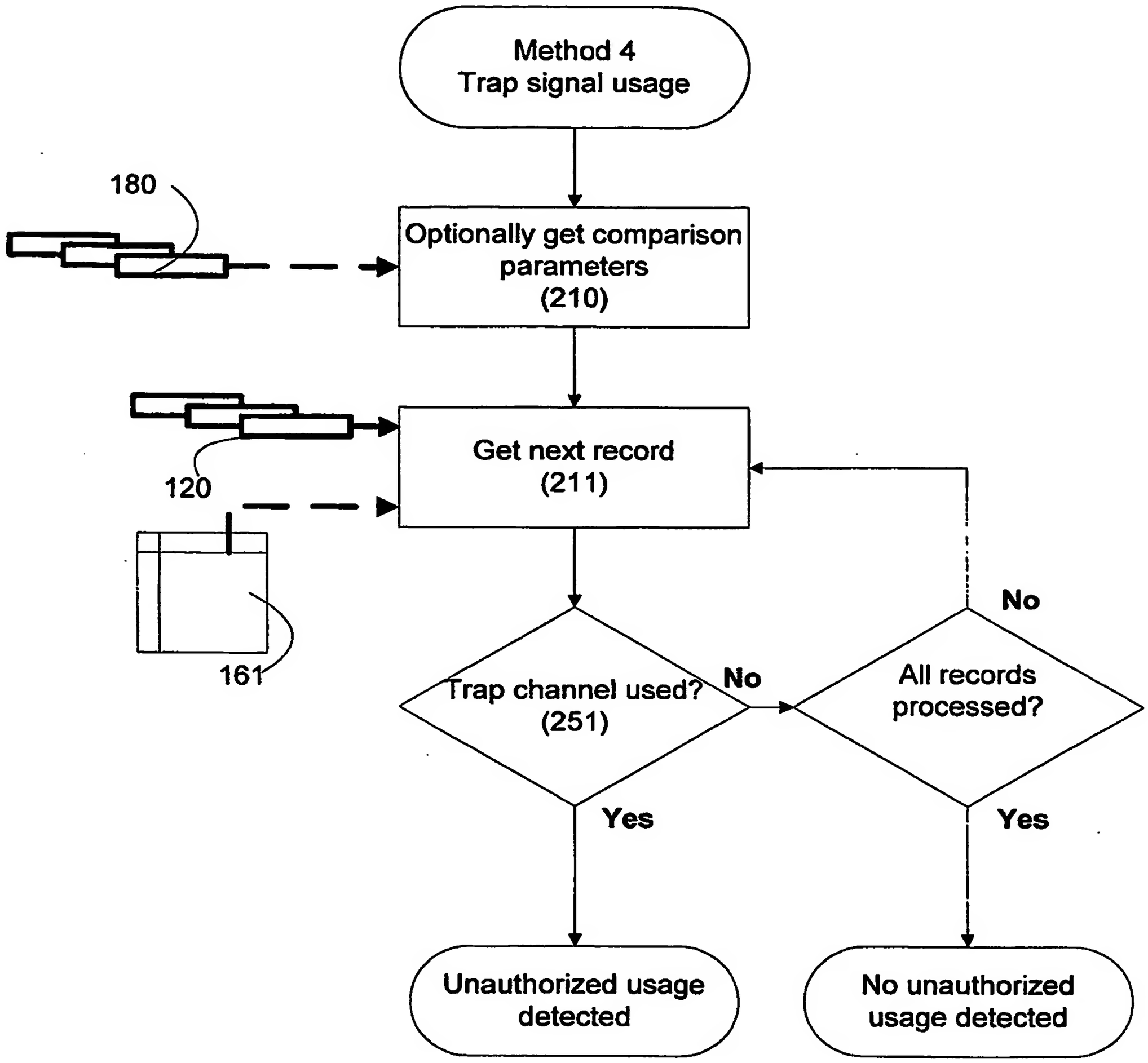

Method 4
Trap signal usage
180
Optionally get comparison parameters (210)
120
Get next record (211)
161
Trap channel used? (251)
No
All records processed?
No
Yes
Yes
Unauthorized usage detected
No unauthorized usage detected

Fig. 10

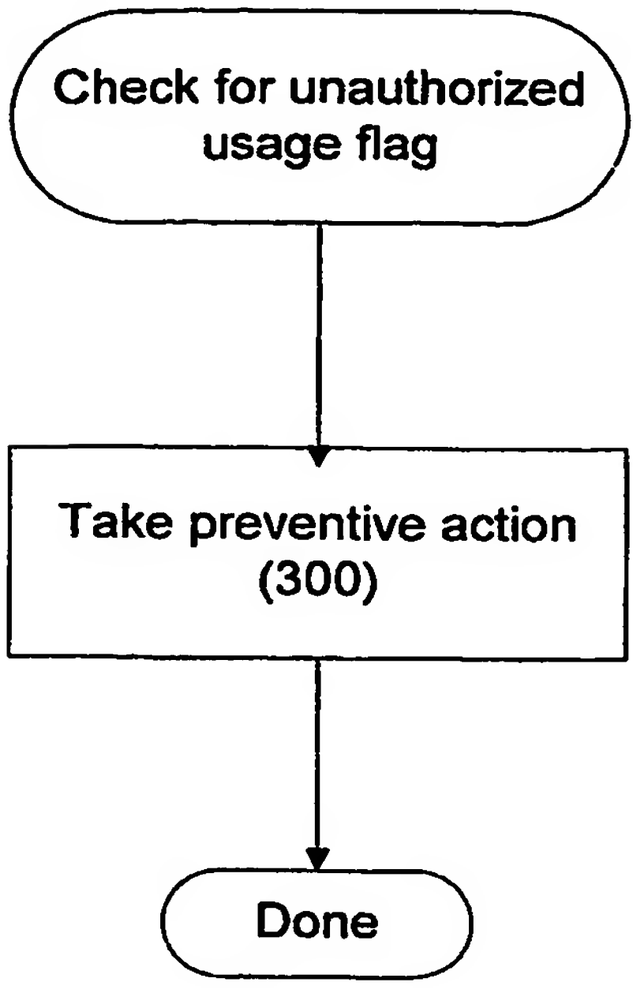

Check for unauthorized usage flag
Take preventive action (300)
Done

Fig. 11

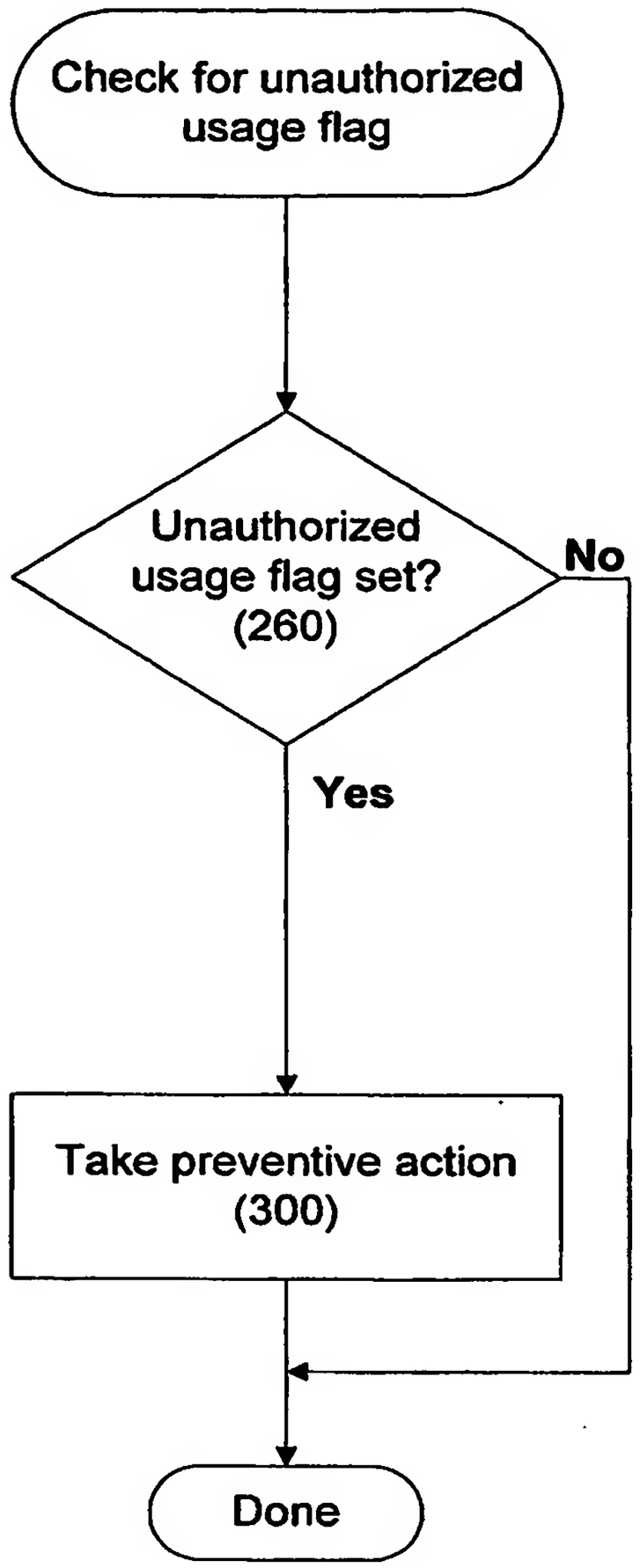

Check for unauthorized usage flag
Unauthorized usage flag set? (260)
No
Yes
Take preventive action (300)
Done

Fig. 12

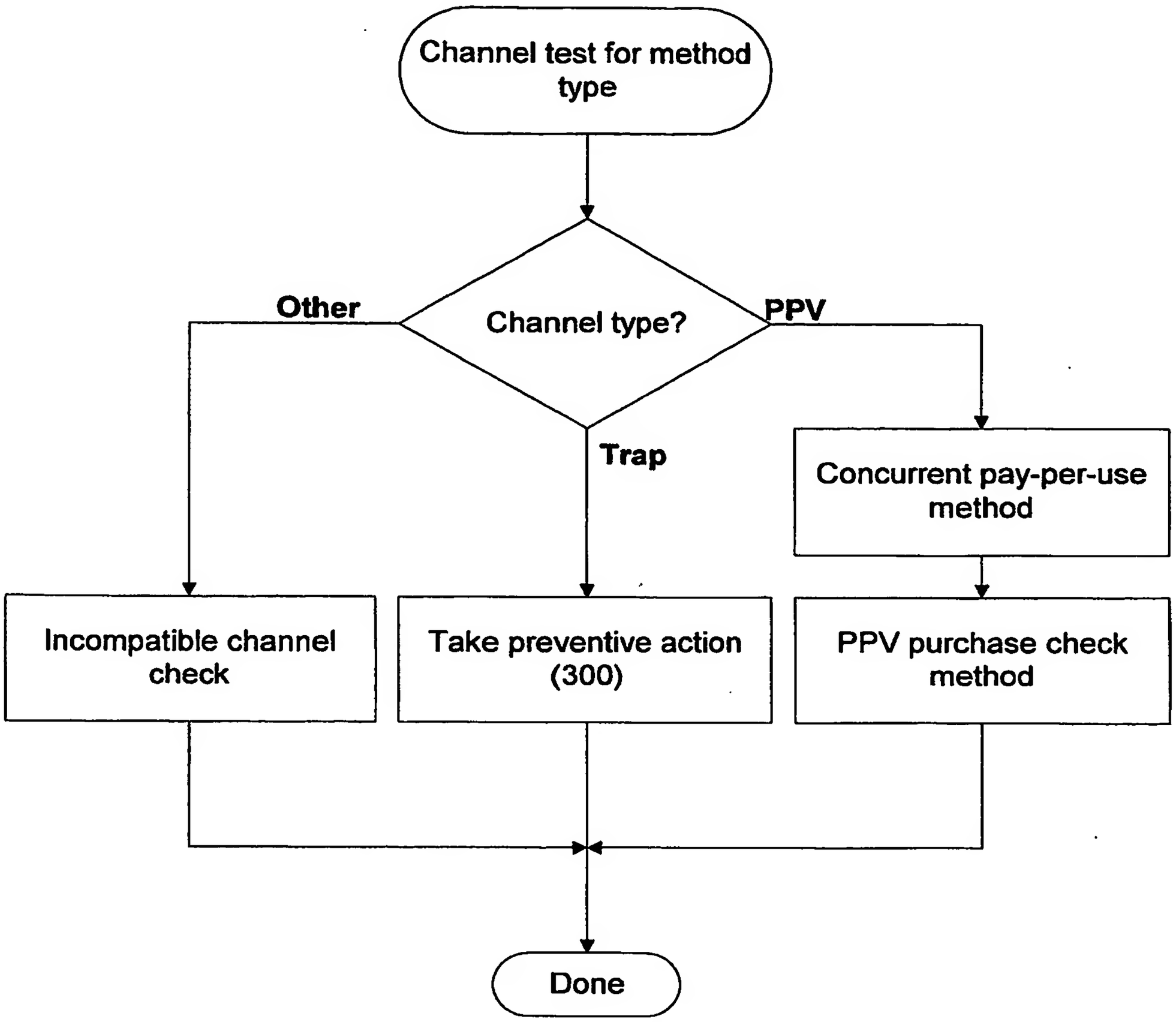

Channel test for method type
Channel type?
Other
Trap
PPV
Concurrent pay-per-use method
Incompatible channel check
Take preventive action (300)
PPV purchase check method
Done

Fig. 13

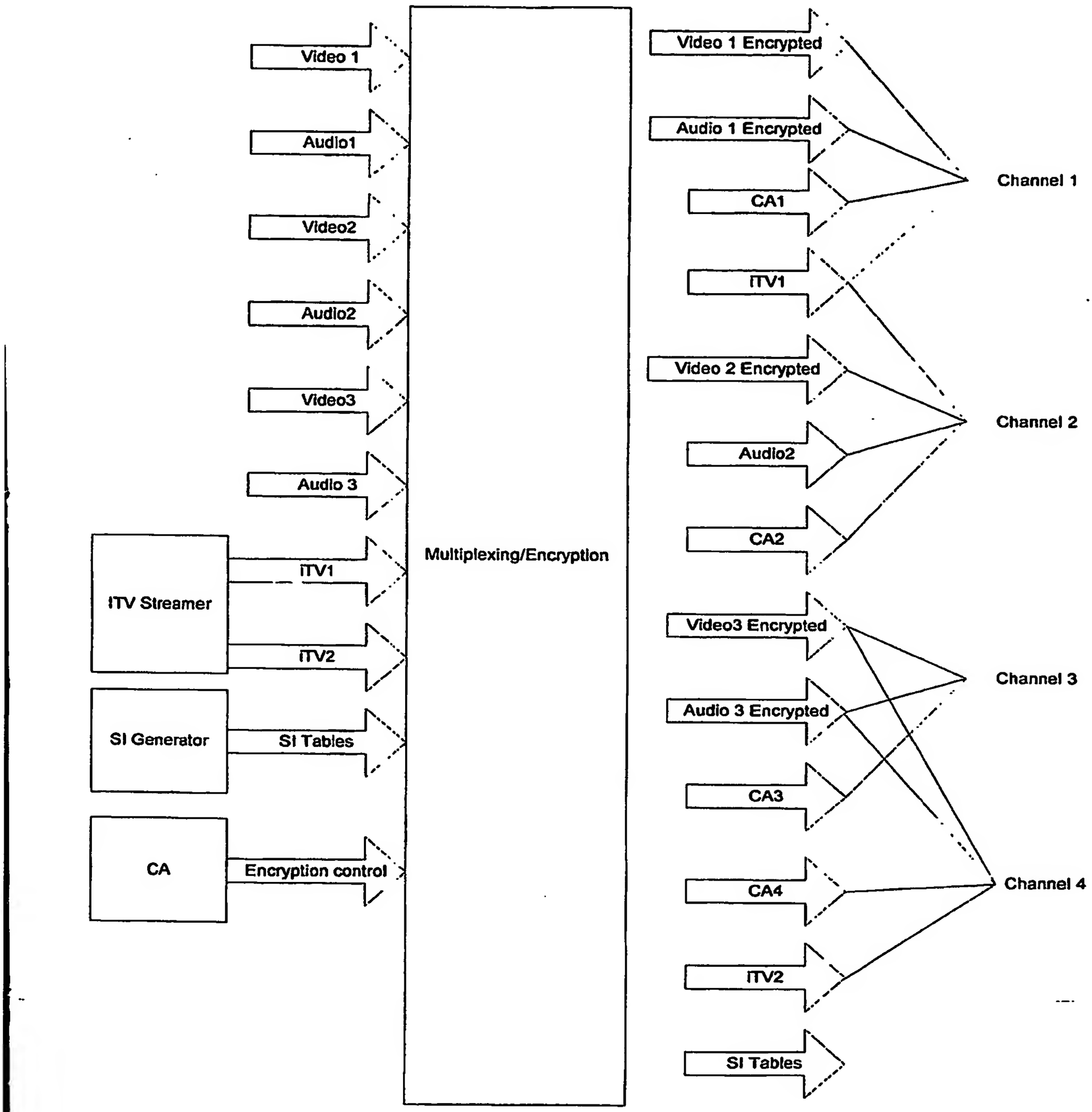

Video 1
Audio1
Video2
Audio2
Video3
Audio 3
ITV Streamer
ITV1
ITV2
SI Generator
SI Tables
CA
Encryption control
Multiplexing/Encryption
Video 1 Encrypted
Audio 1 Encrypted
CA1
Channel 1
ITV1
Video 2 Encrypted
Audio2
CA2
Channel 2
Video3 Encrypted
Audio 3 Encrypted
CA3
CA4
Channel 3
Channel 4
ITV2
SI Tables

Fig. 14

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/CA04/001831

International filing date: 15 October 2004 (15.10.2004)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/511,790
Filing date: 16 October 2003 (16.10.2003)

Date of receipt at the International Bureau: 02 March 2005 (02.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record.

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.